(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－152196
（P2002－152196A）
(43)公開日　平成14年５月24日(2002.5.24)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　9/32		Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０		６６０Ｄ	５Ｋ０６７
	６６０	Ｈ０４Ｌ　9/00	６７５Ｂ	
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｓ	

審査請求　有　　請求項の数35　ＯＬ　（全 43 頁）

(21)出願番号　特願2001－250922(P2001－250922)

(22)出願日　平成13年８月22日(2001.8.22)

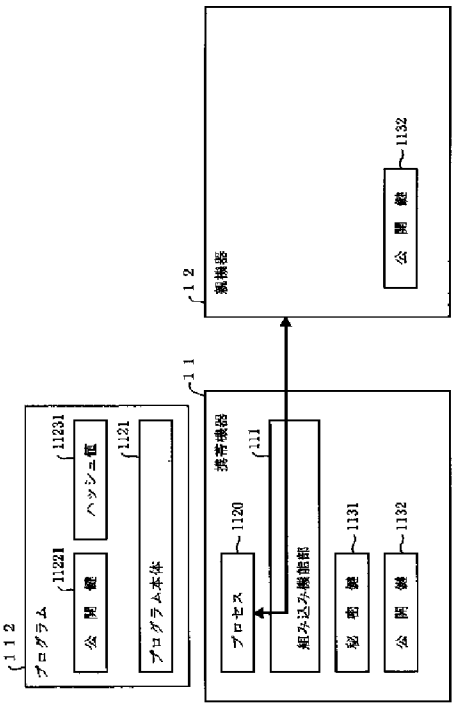
(31)優先権主張番号　特願2000－264850(P2000－264850)
(32)優先日　平成12年９月１日(2000.9.1)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　市瀬　規善
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100088890
弁理士　河原　純一

Ｆターム(参考)　5J104 AA07 AA08 AA09 KA02 KA05
KA21 LA03 LA05 LA06 NA02
NA12 PA02
5K067 AA32 BB04 DD17 DD23 EE02
EE10 HH22 HH23 HH24

(54)【発明の名称】　秘密鍵なしプログラム認証方法，プログラムＩＤ通信処理制御方法、プログラムＩＤ通信範囲制御方法および公開鍵毎通信路提供方法

(57)【要約】
【課題】　読み出し改竄可でよい環境での、通信における成りすましを防止する。
【解決手段】携帯機器１１が、組み込み機能部１１１により、ハッシュ値１１２３１がプログラム本体１１２１とプログラム１１２の出所由来を表す公開鍵１１２２１と対をなす秘密鍵とによって生成されたものであることを確認する。親機器１２が、公開鍵１１２３２および秘密鍵１１３１を用いた公開鍵方式により携帯機器１１の認証を行い、認証が成功した場合に、携帯機器１１によるハッシュ値確認結果に基づいてプログラム１１２が真正な出所由来をもつものかを判定する。親機器１２が携帯機器１１の認証に成功し、かつプログラム１１２が真正な出所由来をもつものであるときに、公開鍵１１２２１でプログラム１１２を認証したとする。



1

【特許請求の範囲】

【請求項１】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が該公開鍵を前記プログラムの出所由来を表すと認証する工程とを含むことを特徴とする秘密鍵なしプログラム認証方法。

【請求項２】　前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする請求項１記載の秘密鍵なしプログラム認証方法。

【請求項３】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする請求項１または２記載の秘密鍵なしプログラム認証方法。

2

【請求項４】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項１または２記載の秘密鍵なしプログラム認証方法。

【請求項５】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が１つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の各公開鍵を、前記プログラムの出所由来を表すと認証する工程とを含むこと

を特徴とする秘密鍵なしプログラム認証方法。

【請求項６】　前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認した署名に対応する公開鍵の集まりを得る工程において、各署名が前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする請求項５記載の秘密鍵なしプログラム認証方法。

【請求項７】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする請求項５または６記載の秘密鍵なしプログラム認証方法。

【請求項８】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項５または６記載の秘密鍵なしプログラム認証方法。

【請求項９】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体と、該プログラムの出所由来を表すＩＤ群とを含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プロセスの元となるプログラムの出所由来を表すＩＤ群の一部または全部を得る工程と、前記出所由来を表すＩＤが１つ以上得られたときに、前記通信・処理装置が前記プログラムを元に生成されたプロセスの処理により前記プログラム実行・通信装置と通信を行う工程と、通信によって発生した処理において、前記通信・処理装置が、前記プログラム実行・管理装置から得られた前記出所由来を表すＩＤ群を元にしたアクセス制御を行う工程とを含むことを特徴とするプログラムＩＤ通信処理制御方法。

【請求項１０】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，該プログラムの出所由来を表す公開鍵，および該公開鍵と対をなす秘密鍵を含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置から該プログラム実行・通信装置に通信をさせるプロセスの元となる前記プログラムの出所由来を表す公開鍵を得る工程と、前記通信・処理装置が、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程と、前記プログラムが認証されたときに、前記通信・処理装置が、前記公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とするプログラムＩＤ通信処理制御方法。

【請求項１１】　前記通信・処理装置が、得られた公開鍵について、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記プログラム実行・通信装置が、前記公開鍵を前記通信・処理装置に送り、前記通信・処理装置が、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置が、該文字列を前記秘密鍵で暗号化した文字列を前記通信・処理装置に送り返し、前記通信・処理装置が、暗号化された文字列を前記送られてきた公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラムを認証することを特徴とする請求項１０記載のプログラムＩＤ通信処理制御方法。

【請求項１２】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プロ

グラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置から前記プログラムの出所由来を表す公開鍵を得、該公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とするプログラムＩＤ通信処理制御方法。

【請求項１３】　前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする請求項１２記載のプログラムＩＤ通信処理制御方法。

【請求項１４】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする請求項１２または１３記載のプログラムＩＤ通信処理制御方法。

【請求項１５】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項１２または１３記載のプログラムＩＤ通信処理制御方法。

【請求項１６】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が１つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の公開鍵の集まりの一部または全部を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とするプログラムＩＤ通信処理制御方法。

【請求項１７】　前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合

わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を各公開鍵でそれぞれ復号した各ダイジェストと、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングして得られるダイジェストとが一致するかどうかを判定することを特徴とする請求項１６記載のプログラムＩＤ通信処理制御方法。

【請求項１８】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする請求項１６または１７記載のプログラムＩＤ通信処理制御方法。

【請求項１９】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項１６または１７記載のプログラムＩＤ通信処理制御方法。

【請求項２０】　プログラムと、これらプログラムを元にプロセスをそれぞれ生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，および該プログラムの出所由来を表すＩＤ群を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表すＩＤ群の一部または全部を得る工程と、前記出所由来を表すＩＤ群が得られたときに、両プログラム実行・通信装置が、得られた出所由来を表すＩＤ群と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表すＩＤ群とを比較し、一致する前記プログラムの出所由来を表すＩＤが１つ以上存在すれば通信路を開く工程とを含むことを特徴とするプログラムＩＤ通信範囲制御方法。

【請求項２１】　プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，該プログラムの出所由来を表す公開鍵，および該公開鍵と対をなす秘密鍵を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置から相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵をそれぞれ得る工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程と、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致し、かつ相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証されたときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とするプログラムＩＤ通信範囲制御方法。

【請求項２２】　両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、両プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵を相手プログラム実行・通信装置に送り、相手プログラム実行・通信装置にランダムな文字列をそれぞれ送り、相手プログラム実行・通信装置が、該文字列を相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した文字列を自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置が、暗号化された文字列を対応する公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置通信装置内のプロセスの元となるプ

ログラムを認証することを特徴とする請求項２１記載のプログラムＩＤ通信範囲制御方法。

【請求項２３】　プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記通信を行う前に、前記公開鍵を相手プログラム実行・通信装置に伝える工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証され、かつ相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致したときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とするプログラムＩＤ通信範囲制御方法。

【請求項２４】　両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、両プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする請求項２３または２４記載のプログラムＩＤ通信範囲制御方法。

【請求項２５】　両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の１つ以上の公開鍵とが一致するかどうかを判定することを特徴とする請求項２３または２４記載のプログラムＩＤ通信範囲制御方法。

【請求項２６】　両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする請求項２３または２４記載のプログラムＩＤ通信範囲制御方法。

【請求項２７】　両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の１つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする請求項２６記載のプログラムＩＤ通信範囲制御方法。

【請求項２８】　プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、各プログラムを元に生成および実行されるプロセスとを含み、各プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を

組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりを相手プログラム実行・通信装置に伝え、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりと相手プログラム実行・通信装置による署名確認結果の公開鍵の集まりとに一致する公開鍵があるかどうかを判定する工程と、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵が１つ以上あるときに、両プログラム実行・通信装置が、プロセス間の通信路を開く工程とを含むことを特徴とするプログラムＩＤ通信範囲制御方法。

【請求項２９】　両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを判定する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、相手プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群で作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする請求項２８記載のプログラムＩＤ通信範囲制御方法。

【請求項３０】　両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の１つ以上の公開鍵とが一致するかどうかを判定することを特徴とする請求項２８または２９記載のプログラムＩＤ通信範囲制御方法。

【請求項３１】　両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする請求項２８または２９記載のプログラムＩＤ通信範囲制御方法。

【請求項３２】　両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が１つ以上得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の１つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする請求項３１記載のプログラムＩＤ通信範囲制御方法。

【請求項３３】　仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする請求項２７または３２記載のプログラムＩＤ通信範囲制御方法。

【請求項３４】　プログラムと、該プログラムを元にプロセスを生成し実行および通信するプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に１つ以上存在する仮想通信路用資源と、１つ以上の通信路用資源とを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により通信を行う際に、出所由来を表す公開鍵と要求された仮想通信路用資源とを対にして仮想通信路と対応させ、仮想通信路を使い通信路を提供する工程をを含むことを特徴とする公開鍵毎通信路提供方法。

【請求項３５】　仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする請求項３４記載の公開鍵毎通信路提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はプログラム認証方法，分散環境におけるプログラム間通信により発生する処理のアクセス制御方法，および分散環境におけるプログラムの通信範囲制御方法に関する。

【０００２】

【従来の技術】従来の情報システムの一例は、たとえば図１９に示すように、プログラム本体１０１２１，およびプログラム１０１２の出所由来を表す公開鍵群１０１２２１～１０１２２ｎと秘密鍵群１０１２４１～１０１２４ｎとの対により構成されるプログラム１０１２と、プログラム実行・通信装置である携帯機器１０１によりプログラム１０１２を元に生成および実行されるプロセス１０１２０により構成される、プログラム１０１２を対象としプログラム１０１２を元にプロセス１０１２０を生成し実行する携帯機器１０１と、携帯機器１０１と通信を行う通信・処理装置である親機器１０２とにより、その主要部が構成されていた。

【０００３】従来の情報システムの一例は、たとえば図１９に示すように、プログラム１０１２と、プログラム１０１２を元にプロセス１０１２０を生成し実行するプログラム実行・通信装置である携帯機器１０１と、携帯機器１０１と通信を行う通信・処理装置である親機器１０２とから、その主要部が構成されていた。

【０００４】プログラム１１２は、プログラム本体１０１２１と、プログラム１０１２の出所由来を表す公開鍵群１０１２２１～１０１２２ｎと、公開鍵群１０１２２１～１０１２２ｎと対をなす秘密鍵群１０１２４１～１０１２４ｎとを含んで構成されていた。

【０００５】携帯機器１０１は、組み込み機能部１０１１と、プログラム１０１２を実行するプロセス１０１２０と、携帯機器１０１に付随する公開鍵１０１３２と、公開鍵１０１３２と対をなす秘密鍵１０１３１と、ユーザ・パスワード情報１０１９０とから構成されていた。

【０００６】親機器１０２は、通信してよい相手を表すＩＤである携帯機器１０１に付随する公開鍵１０１３２と、通信してよいユーザを表すユーザ・パスワード情報１０１９０とを含んで構成されていた。

【０００７】このような従来の情報システムでは、プログラム１０１２を元に生成されたプロセス１０１２０の処理により携帯機器１０１が親機器１０２と通信を行う以前に、親機器１０２が、携帯機器１０１から携帯機器１０１に通信をさせるプロセス１０１２０の元となるプログラム１０１２の出所由来を表す公開鍵１０１２２１～１０１２２ｎを得る工程と、親機器１０２が、得られた各公開鍵１０１２２１～１０１２２ｎについて、携帯機器１０１に通信をさせるプロセス１０１２０の元となるプログラム１０１２の出所由来を表す公開鍵群１０１２２１～１０１２２ｎおよび秘密鍵群１０１２４１～１０１２４ｎを用いさせて認証を行うことで、プロセス１０１２０の元となるプログラム１０１２が認証に成功した公開鍵すべてをもつと認証を行っていた。

【０００８】また、従来、情報システムの他の例は、たとえば図２０に示すように、プログラム１０１２と、プログラム１０１２を元にプロセス１０１２０を生成し実行するプログラム実行・通信装置である携帯機器１０１と、携帯機器１０１と通信を行う通信・処理装置である親機器１０２とから、その主要部が構成されていた。

【０００９】携帯機器１０１は、組み込み機能部１０１１と、プログラム１０１２を実行するプロセス１０１２０と、携帯機器１０１に付随する公開鍵１０１３２および秘密鍵１０１３１と、ユーザ・パスワード情報１０１９０とから構成されていた。

【００１０】親機器１０２は、通信してよい相手を示す公開鍵としての携帯機器１０１に付随する公開鍵１０１３２と、ユーザ・パスワード情報１０１９０とをもつ。

【００１１】このような従来の情報システムでは、携帯機器１０１で、ユーザ・パスワード情報１０１９０について認証を行い、プログラム１０１２を実行するプロセス１０１２０がユーザ・パスワード情報１０１９０を保持する。プロセス１０１２０が親機器１０２と通信をしようとして通信要求が発生した場合、親機器１０２は、携帯機器１０１から公開鍵１０１３２を受け取り、公開鍵１０１３２と一致するものであれば、携帯機器１０１に対し公開鍵１０１３２について認証を行い、認証に成功した場合は、携帯機器１０１内のプログラム１０１２を実行するプロセス１０１２０と親機器１０２との通信を許し、またその通信によって発生する処理についてのアクセス制御は、通信相手によらず同じアクセス制御を行うか、または通信相手のプロセス１０１２０のもつユーザ・パスワード情報１０１９０を引き継ぎ、ユーザ認証が成功すればそれをもとにアクセス制御を行っていた。

【００１２】さらに、従来、情報システムの別の例は、たとえば図２１に示すように、携帯機器１０１と、親機器１０２とから、その主要部が構成されていた。

【００１３】携帯機器１０１は、組み込み機能部１０１１と、プログラム１０１２と、プログラム１０１２を実行するプロセス１０１２０と、携帯機器１０１に付随する秘密鍵１０１３１と、秘密鍵１０１３１と対をなす公開鍵１０１３２と、通信してよい相手を示す公開鍵１０２３２とを含んで構成されていた。

【００１４】親機器１０２は、組み込み機能部１０２１

と、プログラム１０２２と、プログラム１０２２を実行するプロセス１０２２０と、親機器１０２に付随する秘密鍵１０２３１と、秘密鍵１０２３１と対を成す公開鍵１０２３２と、通信してよい相手を示す公開鍵１０１３２とから構成されていた。

【００１５】このような従来の情報システムでは、プロセス１０１２０とプロセス１０２２０とが通信をしようとして通信要求が発生した場合、組み込み機能部１０１１および１０２１は、まず、公開鍵１０１３２および１０２３２を互いに渡し、受け取った公開鍵１０２３２および１０１３２と通信してよい相手を示す公開鍵１０２３２および１０１０３２とをそれぞれ比較する。一致すれば、各組み込み機能部１０１１および１０２１は、受け取った公開鍵１０２３２および１０１３２で相互認証を行い、相互認証が成功すれば、プロセス１０１２０とプロセス１０２２０との通信を許す。一方、受け取った公開鍵１０２３２および１０１３２と通信してよい相手を示す公開鍵１０１３３および１０２３３とが異なるか、公開鍵１０２３２および１０１３２での相互認証が失敗した場合は、プロセス１０１２０とプロセス１０２２０との間の通信を許さなかった。また通信路資源群を仮想的に公開鍵毎に別資源として提供していなかった。

【００１６】

【発明が解決しようとする課題】第１の問題点は、通信時の成りすましを防ぐためには、プログラムが存在するエリア（メモリ，ディスク等）のセキュリティレベルとして、読み出し改竄不可でなければならないということである。その理由は、プログラムが秘密鍵をもつ必要があるからである。

【００１７】第２の問題点は、分散環境において、ユーザ・パスワード情報に類する共通の情報を保持し、維持管理する必要があることである。その理由は、認証するために同じユーザ・パスワード情報に類する情報を共有する必要があるからである。

【００１８】第３の問題点は、ユーザ・パスワード情報に類する情報を利用しない場合は、通信相手によらず皆同じ権限で処理を実行させることである。その理由は、アクセス制御をするための正当性を保証できる情報を得られないからである。

【００１９】第４の問題点は、機器，プログラムないしはシステムの設計時に機器，プログラムないしはプロセスの通信すべき相手をどのプログラムとするかを個別に設計しなければならないということである。その理由は、通信相手は通信すべき相手がもつているはずの公開鍵の設定によって決まるからである。

【００２０】第５の問題点は、システムの拡張および複数のシステムの乗り入れの際の手間が多いということである。その理由は、システムの拡張および複数のシステムの乗り入れのための、機器，プログラムないしはシステムの設計時に機器，プログラムないしはプロセスの通信すべき相手をどのプログラムとするかを個々に設計し直さなければならないからである。

【００２１】第６の問題点は、システムが特定のサービスに固定したものになりがちであることである。その理由は、システムの拡張および複数のシステムの乗り入れの際の手間が多いからである。

【００２２】第７の問題点は、どの通信路をどの公開鍵に対応し利用するか設計、管理する必要があることである。その理由は、通信路資源群を仮想的に公開鍵毎に別資源として提供していなかったからである。

【００２３】本発明の第１の目的は、プログラムが存在するエリアのセキュリティレベルとして、読み出し改竄可でよい環境での、通信における成りすましを防止する秘密鍵なしプログラム認証方法を提供することにある。

【００２４】本発明の第２の目的は、集中管理下にない分散環境におけるプログラム間通信により発生する処理のアクセス制御を行うためのプログラムＩＤ通信処理制御方法を提供することにある。

【００２５】本発明の第３の目的は、分散環境において、通信の範囲、つまり情報の流通について範囲が予め限定されており、通信範囲に関するシステム設計が容易なプログラムＩＤ通信範囲制御方法を提供することにある。

【００２６】本発明の第４の目的は、公開鍵別の通信を行う場合に、どの通信路がどの公開鍵用で占有されるかが予め限定されており、通信路に関するシステム設計が容易な公開鍵毎通信路提供方法を提供することにある。

【００２７】なお、先行技術文献として特開２０００－１４８４６９があるが、この公報に開示された「モジュラーアプリケーション間のサービスへのアクセス制御」方法は、第１のコンピュータプログラムモジュールが第２のコンピュータプログラムモジュールからサービスのアクセスを与える権力をデジタル的に署名されたかどうかを判定し、デジタル的に署名された場合に第１のコンピュータプログラムモジュールにサービスへのアクセスを提供するようにしたものである。しかし、この方法は、第１のコンピュータプログラムモジュールが第２のコンピュータプログラムモジュールからのサービスにアクセスできるように、第１のコンピュータプログラムモジュールおよび第２のコンピュータプログラムモジュールを同じコンピューティングノード上の同じアドレス空間内で実行させることができるようにするためのものであり、本発明のように異なるプログラム実行・通信装置上で異なるプログラムを通信を介して協働させるようにするためのものではない。

【００２８】

【課題を解決するための手段】本発明の秘密鍵なしプログラム認証方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処

理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が該公開鍵を前記プログラムの出所由来を表すと認証する工程とを含むことを特徴とする。

【００２９】また、本発明の秘密鍵なしプログラム認証方法は、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする。

【００３０】さらに、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする。

【００３１】さらにまた、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【００３２】また、本発明の秘密鍵なしプログラム認証方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が１つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の各公開鍵を、前記プログラムの出所由来を表すと認証する工程とを含むことを特徴とする。

【００３３】さらに、本発明の秘密鍵なしプログラム認証方法は、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて

作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認した署名に対応する公開鍵の集まりを得る工程において、各署名が前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする。

【００３４】さらにまた、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする。

【００３５】また、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【００３６】一方、本発明のプログラムＩＤ通信処理制御方は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体と、該プログラムの出所由来を表すＩＤ群とを含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プロセスの元となるプログラムの出所由来を表すＩＤ群の一部または全部を得る工程と、前記出所由来を表すＩＤが１つ以上得られたときに、前記通信・処理装置が前記プログラムを元に生成されたプロセスの処理により前記プログラム実行・通信装置と通信を行う工程と、通信によって発生した処理において、前記通信・処理装置が、前記プログラム実行・管理装置から得られた前記出所由来を表すＩＤ群を元にしたアクセス制御を行う工程とを含むことを特徴とする。

【００３７】また、本発明のプログラムＩＤ通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，該プログラムの出所由来を表す公開鍵，および該公開鍵と対をなす秘密鍵を含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置から該プログラム実行・通信装置に通信をさせるプロセスの元となる前記プログラムの出所由来を表す公開鍵を得る工程と、前記通信・処理装置が、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程と、前記プログラムが認証されたときに、前記通信・処理装置が、前記公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とする。

【００３８】さらに、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、得られた公開鍵について、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記プログラム実行・通信装置が、前記公開鍵を前記通信・処理装置に送り、前記通信・処理装置が、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置が、該文字列を前記秘密鍵で暗号化した文字列を前記通信・処理装置に送り返し、前記通信・処理装置が、暗号化された文字列を前記送られてきた公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラムを認証することを特徴とする。

【００３９】さらにまた、本発明のプログラムＩＤ通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元

に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置から前記プログラムの出所由来を表す公開鍵を得、該公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とする。

【００４０】また、本発明のプログラムＩＤ通信処理制御方法は、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする。

【００４１】さらに、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする。

【００４２】さらにまた、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【００４３】また、本発明のプログラムＩＤ通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が１つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の公開鍵の集まりの一部または全部を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とする。

【００４４】さらに、本発明のプログラムＩＤ通信処理制御方法は、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせ

て作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を各公開鍵でそれぞれ復号した各ダイジェストと、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングして得られるダイジェストとが一致するかどうかを判定することを特徴とする。

【００４５】さらにまた、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする。

【００４６】また、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【００４７】他方、本発明のプログラムＩＤ通信範囲制御方法は、プログラムと、これらプログラムを元にプロセスをそれぞれ生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，および該プログラムの出所由来を表すＩＤ群を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表すＩＤ群の一部または全部を得る工程と、前記出所由来を表すＩＤ群が得られたときに、両プログラム実行・通信装置が、得られた出所由来を表すＩＤ群と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表すＩＤ群とを比較し、一致する前記プログラムの出所由来を表すＩＤが１つ以上存在すれば通信路を開く工程とを含むことを特徴とする。

【００４８】また、本発明のプログラムＩＤ通信範囲制御方法は、プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，該プログラムの出所由来を表す公開鍵，および該公開鍵と対をなす秘密鍵を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置から相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵をそれぞれ得る工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程と、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致し、かつ相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証されたときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とする。

【００４９】また、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、両プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵を相手プログラム実行・通信装置に送り、相手プログラム実行・通信装置にランダムな文字列をそれぞれ送り、相手プログラム実行・通信装置が、該文字列を相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した文字列を自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置が、暗号化された文字列を対応する公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置通信装置内のプロセスの元となるプログラ

ムを認証することを特徴とする。

【００５０】さらに、本発明のプログラムＩＤ通信範囲制御方法は、プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記通信を行う前に、前記公開鍵を相手プログラム実行・通信装置に伝える工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証され、かつ相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致したときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とする。

【００５１】さらにまた、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、両プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする。

【００５２】また、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の１つ以上の公開鍵とが一致するかどうかを判定することを特徴とする。

【００５３】さらに、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする。

【００５４】さらにまた、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の１つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする。

【００５５】また、本発明のプログラムＩＤ通信範囲制御方法は、プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、各プログラムを元に生成および実行されるプロセスとを含み、各プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵

群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりを相手プログラム実行・通信装置に伝え、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりと相手プログラム実行・通信装置による署名確認結果の公開鍵の集まりとに一致する公開鍵があるかどうかを判定する工程と、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵が１つ以上あるときに、両プログラム実行・通信装置が、プロセス間の通信路を開く工程とを含むことを特徴とする。

【００５６】さらに、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを判定する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、相手プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群で作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする。

【００５７】さらにまた、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の１つ以上の公開鍵とが一致するかどうかを判定することを特徴とする。

【００５８】また、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする。

【００５９】さらに、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が１つ以上得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の１つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする。

【００６０】さらにまた、本発明のプログラムＩＤ通信範囲制御方法は、仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする。

【００６１】一方、本発明の公開鍵毎通信路提供方法は、プログラムと、該プログラムを元にプロセスを生成し実行および通信するプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に１つ以上存在する仮想通信路用資源と、１つ以上の通信路用資源とを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により通信を行う際に、出所由来を表す公開鍵と要求された仮想通信路用資源とを対にして仮想通信路と対応させ、仮想通信路を使い通信路を提供する工程をを含むことを特

徴とする。

【００６２】さらにまた、本発明の公開鍵毎通信路提供方法は、仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする。

【００６３】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【００６４】（１）第１の実施の形態

図１を参照すると、本発明の第１の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器１１と、通信機能を有する通信・処理装置が適用された親機器１２と、携帯機器１１にインストールされて実行されるプログラム１１２とから、その主要部が構成されている。

【００６５】実行機能および通信機能は、Ｊａｖａ（サンマイクロシステムズ社の登録商標）などが想定される。

【００６６】携帯機器１１としては、携帯電話機（ＰＨＳ（Ｐｅｒｓｏｎａｌ　ＨａｎｄｙＰｈｏｎｅ）を含む），携帯情報端末等が想定される。

【００６７】親機器１２としては、ＰＯＳ（Ｐｏｉｎｔ　Ｏｆ　Ｓａｌｅｓ）端末等が想定される。

【００６８】携帯機器１１と親機器１２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ），ＰＩＡＦＳ（ＰＨＳ　Ｉｎｔｅｒｎｅｔ　Ａｃｃｅｓｓ　Ｆｏｒｕｍ　Ｓｔａｎｄａｒｄ）等の近距離無線通信技術で実現されるものとする。

【００６９】携帯機器１１は、信頼できる組み込み機能部１１１と、プログラム１１２を実行するプロセス１１２０と、携帯機器１１に付随する秘密鍵１１３１および公開鍵１１３２とを含んで構成されている。

【００７０】プログラム１１２は、プログラム本体１１２１と、プログラム１１２の出所由来を表す公開鍵１１２２１と、プログラム本体１１２１をハッシュ関数でハッシングしたダイジェストを公開鍵１１２２１と対をなす秘密鍵（図示せず）で暗号化した署名（デジタル署名，電子署名）であるハッシュ値１１２３１とを含んで構成されている。なお、プログラム１１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体１１２１，公開鍵１１２２１，およびハッシュ値１１２３１が一体として作成されている。

【００７１】親機器１２は、通信してよい相手を示す公開鍵として、携帯機器１１に付随する公開鍵１１３２をもつ。

【００７２】図２を参照すると、携帯機器１１の組み込み機能部１１１および親機器１２の処理は、ハッシュ値確認ステップＳ１０１と、通信要求発生ステップＳ１０２と、携帯機器認証ステップＳ１０３と、プログラム出所由来判定ステップＳ１０４と、プログラム認証ステップＳ１０５と、プログラム不認証ステップＳ１０６とからなる。

【００７３】次に、このように構成された第１の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの動作について、図１および図２を参照して詳細に説明する。

【００７４】まず、携帯機器１１は、組み込み機能部１１１により、ハッシュ値１１２３１がプログラム本体１１２１および公開鍵１１２２１と対をなす秘密鍵とによって生成されたものであるかどうかを確認する（ステップＳ１０１）。詳しくは、組み込み機能部１１１は、ハッシュ値１１２３１を公開鍵１１２２１で復号してプログラム本体１１２１をハッシングしたダイジェストを得る一方、プログラム本体１１２１を既知のハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値１１２３１がプログラム本体１１２１および公開鍵１１２２１と対をなす秘密鍵とによって生成されたものであるかどうかを確認する。すなわち、プログラム本体１１２１および公開鍵１１２２１が改竄されたものでなく、プログラム１１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器１１にプログラム１１２が導入、たとえばダウンロードされたときに１回行われればよい。

【００７５】次に、携帯機器１１内のプログラム１１２を実行するプロセス１１２０が親機器１２と通信をしようとして通信要求を発生させた場合（ステップＳ１０２）、またはそれ以前に、親機器１２は、携帯機器１１に付随する公開鍵１１３２および秘密鍵１１３１を用いた公開鍵方式により携帯機器１１の認証を行う（ステップＳ１０３）。

【００７６】たとえば、親機器１２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器１１に付随する公開鍵１１３２と、携帯機器１１が保持する携帯機器１１に付随する公開鍵１１３２とが一致するかどうかを判定し、一致した場合に携帯機器１１の認証をおこなう。

【００７７】また、ＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ，Ａｄｌｅｍａｎ）の公開鍵によるワン・タイム・パスワード（Ｏｎｅ　Ｔｉｍｅ　Ｐａｓｓｗｏｒｄ）方式を用いた場合、親機器１２は携帯機器１１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器１１の組み込み機能部１１１はその文字列を携帯機器１１に付随する秘密鍵１１３１で暗号化して親機器１２に送り返し（”Ｒｅｓｐｏｎｓｅ”），親機器１２は暗号化

した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器１１に付随する公開鍵１１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器１１を通信してよい相手（つまり、通信してよい相手を示す公開鍵として保持する携帯機器１１に付随する公開鍵１２３２と対をなす秘密鍵１１３１を所有するもの）であると認証する。

【００７８】携帯機器１１の認証に成功した場合、親機器１２は、携帯機器１１の組み込み機能部１１１から携帯機器１１によるハッシュ値確認結果の公開鍵１１２２１を得、携帯機器１１によるハッシュ値確認結果に基づいてプログラム１１２が真正な出所由来をもつものであるかどうかを判定し（ステップＳ１０４）、そうであれば得られた公開鍵１１２２１でプログラム１１２を認証したとする（ステップＳ１０５）。

【００７９】一方、携帯機器１１の認証に失敗した場合（ステップＳ１０３）、または公開鍵１１２２１がプログラム１１２の真正な出所由来を表す公開鍵でなかった場合（ステップＳ１０４）、親機器１２は、プログラム１１２を認証しない。

【００８０】第１の実施の形態によれば、プログラム１１２が秘密鍵をもたなくても、親機器１２は、親機器１２と通信をしようとしてきた携帯機器１１内のプロセス１１２０の元となるプログラム１１２の認証が可能であることから、盗み見や改竄が可能な環境下にあるプログラム１１２を元にして動作する携帯機器１１と通信を行う場合に、親機器１２がプログラム１１２の成りすましを防止しかつ認証を行うことができる。

【００８１】（２）　第２の実施の形態

図３を参照すると、本発明の第２の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器２１と、通信機能を有する通信・処理装置が適用された親機器２２と、携帯機器２１にインストールされて実行されるプログラム２１２とから、その主要部が構成されている。

【００８２】実行機能および通信機能は、Ｊａｖａなどが想定される。

【００８３】携帯機器２１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【００８４】親機器２２としては、ＰＯＳ端末等が想定される。

【００８５】携帯機器２１と親機器２２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【００８６】携帯機器２１は、信頼できる組み込み機能部２１１と、プログラム２１２を実行するプロセス２１２０と、携帯機器２１に付随する秘密鍵２１３１および公開鍵２１３２とを含んで構成されている。

【００８７】プログラム２１２は、プログラム本体２１２１と、プログラム２１２の出所由来を表す公開鍵群２１２２１～２１２２ｎ（ｎは2以上の正整数。以下同様）と、プログラム本体２１２１および公開鍵群２１２２１～２１２２ｎを組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵２１２２１～２１２２ｎと対をなす各秘密鍵（図示せず）でそれぞれ暗号化した署名群であるハッシュ値群２１２３１～２１２３ｎとを含んで構成されている。なお、プログラム２１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体２１２１，公開鍵群２１２２１～２１２２ｎ，およびハッシュ値群２１２３１～２１２３ｎが一体として作成されている。

【００８８】親機器２２は、通信してよい相手を示す公開鍵として、携帯機器２１に付随する公開鍵２１３２をもつ。

【００８９】図４を参照すると、携帯機器２１の組み込み機能部２１１および親機器２２の処理は、ハッシュ値確認ステップＳ２０１と、通信要求発生ステップＳ２０２と、携帯機器認証ステップＳ２０３と、プログラム由来判定ステップＳ２０４と、プログラム認証ステップＳ２０５と、プログラム不認証ステップＳ２０６とからなる。

【００９０】次に、このように構成された第２の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの動作について、図３および図４を参照して詳細に説明する。

【００９１】まず、携帯機器２１は、組み込み機能部２１１により、各ハッシュ値２１２３１～２１２３ｎがプログラム本体２１２１および公開鍵群２１２２１～２１２２ｎと各公開鍵２１２２１～２１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップＳ２０１）。詳しくは、組み込み機能部２１１は、各ハッシュ値２１２３１～２１２３ｎを各公開鍵２１２２１～２１２２ｎでそれぞれ復号してプログラム本体２２２１および公開鍵群２１２２１～２１２２ｎを組み合わせて作成されたデータをハッシングしたダイジェスト群を得る一方、プログラム本体２１２１および公開鍵群２１２２１～２１２２ｎを組み合わせて作成されたデータを既知のハッシュ関数でハッシングしてダイジェストを得、該ダイジェストとダイジェスト群の一つ一つとが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値２１２３１～２１２３ｎがプログラム本体２１２１および公開鍵群２１２２１～２１２２ｎと各公開鍵２１２２１～２１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体２１２１および公開鍵群２１２２１～２１２２ｎが、改竄されたものでなく、

プログラム２１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器２１にプログラム２１２が導入、たとえばダウンロードされたときに１回行われればよい。

【００９２】次に、携帯機器２１内のプログラム２１２を実行するプロセス２１２０が親機器２２と通信をしようとして通信要求が発生した場合(ステップＳ２０２)、またはそれ以前に、親機器２２は、携帯機器２１に付随する秘密鍵２１３１および公開鍵２１３２を用いた公開鍵方式により携帯機器２１の認証を行う（ステップＳ２０３）。

【００９３】たとえば、親機器２２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器２１に付随する公開鍵２１３２と、携帯機器２１が保持する携帯機器２１に付随する公開鍵２１３２とが一致するかどうかを判定し、一致した場合に携帯機器２１の認証を行う。

【００９４】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器２２は携帯機器２１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器２１の組み込み機能部２１１はその文字列を携帯機器２１に付随する秘密鍵２１３１で暗号化して親機器２２に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器２２は暗号化した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器２１に付随する公開鍵２１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器２１を通信してよい相手（つまり、通信してよい相手を示す公開鍵として保持する携帯機器２１に付随する公開鍵２１３２と対をなす秘密鍵２１３１を所有するもの）であると認証する。

【００９５】携帯機器２１の認証に成功した場合、親機器２２は、携帯機器２１の組み込み機能部２１１から携帯機器２１によるハッシュ値確認結果の公開鍵の集まりを得、携帯機器２１によるハッシュ値確認結果の公開鍵の集まりに１つ以上の公開鍵が含まれていればプログラム２１２が真正な出所由来をもつものであると判定し（ステップＳ２０４）、公開鍵の集まりの一部または全部でプログラム２１２を認証したとする（ステップＳ２０５）。

【００９６】一方、携帯機器２１の認証に失敗した場合（ステップＳ２０３）、またはプログラム２１２の真正な出所由来を表す公開鍵が得られなかった場合（ステップＳ２０４）、親機器２２は、プログラム２１２を認証しない（ステップＳ２０６）。

【００９７】なお、上記第２の実施の形態では、ステップＳ２０４で携帯機器２１によるハッシュ値確認結果の公開鍵の集まりに１つ以上の公開鍵が含まれていればプログラム２１２が真正な出所由来をもつものであると判定したが、携帯機器２１によるハッシュ値確認結果の公開鍵の集まりに公開鍵群２１２２１～２１２２ｎのすべてが含まれていたときにのみプログラム２１２が真正な出所由来をもつものであると判定するようにすることもできる。

【００９８】第２の実施の形態によれば、プログラム２１２が公開鍵群２１２２１～２１２２ｎをもつことを許す場合は、プログラム本体２１２１とともに保持する公開鍵群２１２２１～２１２２ｎに対し署名群であるハッシュ値群２１２３１～２１２３ｎを付与することから、プログラムの成りすましを防止することができる。

【００９９】（２）第３の実施の形態

図５を参照すると、本発明の第３の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器３１と、通信機能を有する通信・処理装置が適用された親機器３２と、携帯機器３１にインストールされて実行されるプログラム３１２とから、その主要部が構成されている。

【０１００】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１０１】携帯機器３１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１０２】親機器３２としては、ＰＯＳ端末等が想定される。

【０１０３】携帯機器３１と親機器３２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１０４】携帯機器３１は、信頼できる組み込み機能部３１１と、プログラム３１２を実行するプロセス３１２０とを含んで構成されている。

【０１０５】プログラム３１２は、プログラム本体３１２１と、プログラム３１２の出所由来を表す公開鍵３１２２１および秘密鍵３１２４１とを含んで構成されている。なお、プログラム３１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体３１２１，公開鍵３１２２１，および秘密鍵３１２４１が一体として作成されている。

【０１０６】図６を参照すると、携帯機器３１の組み込み機能部３１１および親機器３２の処理は、通信要求発生ステップＳ３０１と、公開鍵獲得ステップＳ３０２と、プログラム認証ステップＳ３０３と、通信・処理ステップＳ３０４と、通信・処理なしステップＳ３０５とからなる。

【０１０７】次に、このように構成された第３の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの動作について、図５および図６を参照して詳細に説明する。

【０１０８】携帯機器３１内のプログラム３１２を実行するプロセス３１２０が親機器３２と通信するための通

信要求を発生させた場合（ステップＳ３０１）、親機器３２は、携帯機器３１の組み込み機能部３１１を介して、プロセス３１２０の元となるプログラム３１２の出所由来を表す公開鍵３１２２１を得る（ステップＳ３０２）。

【０１０９】次に、親機器３２は、携帯機器３１の組み込み機能部３１１に対し、公開鍵３１２２１および秘密鍵３１２４１を用いた公開鍵方式によりプロセス３１２０の元となるプログラム３１２が真正な出所由来をもつものであるかどうかを認証する（ステップＳ３０３）。

【０１１０】たとえば、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器３２は携帯機器３１の組み込み部３１１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器３１の組み込み機能部３１１はその文字列をプロセス３１２０の元となるプログラム３１２の出所由来を表す公開鍵３１２２１と対をなす秘密鍵３１２４１で暗号化して親機器３２に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器３２は暗号化した文字列を先に受け取った公開鍵３１２２１で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、プロセス３１２０の元となるプログラム３１２は真正な出所由来をもつものである（つまり、プログラム３１２が該プログラム３１２の出所由来を表す公開鍵３１２２１と対をなす秘密鍵３１２４１を所有する）と認証する。

【０１１１】プログラム３１２の認証に成功した場合（ステップＳ３０３）、親機器３２は、以降の通信によって発生する処理を、公開鍵３１２２１に対応するユーザ権限でアクセス制御して実行する（ステップＳ３０４）。

【０１１２】一方、プログラム３１２の認証に失敗した場合（ステップＳ３０３）、または公開鍵３１２２１に対応するユーザ権限が存在しない場合、親機器３２は、通信によって発生する処理をしないか、特定の制限されたユーザ権限で処理を実行する（ステップＳ３０５）。

【０１１３】第３の実施の形態によれば、プログラム３１２の出所由来を表す公開鍵３１２２１、つまりプログラム３１２の製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うことから、悪意のプログラムに対しセキュリティを保つことができる。

【０１１４】また、プログラム３１２の出所由来を表す公開鍵３１２２１、つまりプログラム３１２の製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うため、ユーザ管理のような集中管理が困難な分散環境下での通信による処理について、悪意のプログラムに対しセキュリティを保つことができる。

【０１１５】（４）　第４の実施の形態

図７を参照すると、本発明の第４の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器４１と、通信機能を有する通信・処理装置が適用された親機器４２と、携帯機器４１にインストールされ実行されるプログラム４１２とから、その主要部が構成されている。

【０１１６】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１１７】携帯機器４１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１１８】親機器４２としては、ＰＯＳ端末等が想定される。

【０１１９】携帯機器４１と親機器４２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１２０】携帯機器４１は、信頼できる組み込み機能部４１１と、プログラム４１２を実行するプロセス４１２０と、携帯機器４１に付随する秘密鍵４１３１および公開鍵４１３２とを含んで構成されている。

【０１２１】プログラム４１２は、プログラム本体４１２１と、プログラム４１２の出所由来を表す公開鍵４１２２１と、プログラム本体４１２１をハッシュ関数でハッシングしたダイジェストを公開鍵４１２２１と対をなす秘密鍵（図示せず）で暗号化した署名であるハッシュ値４１２３１とを含んで構成されている。なお、プログラム４１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体４１２１，公開鍵４１２２１，およびハッシュ値４１２３１が一体として作成されている。

【０１２２】親機器４２は、通信してよい相手を示す公開鍵として、携帯機器４１に付随する公開鍵４１３２をもつ。

【０１２３】図８を参照すると、携帯機器４１の組み込み機能部４１１および親機器４２の処理は、ハッシュ値確認ステップＳ４０１と、通信要求発生ステップＳ４０２と、携帯機器認証ステップＳ４０３と、プログラム出所由来判定ステップＳ４０４と、通信・処理ステップＳ４０５と、通信・処理なしステップＳ４０６とからなる。

【０１２４】次に、このように構成された第４の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの動作について、図７および図８を参照して詳細に説明する。

【０１２５】まず、携帯機器４１は、組み込み機能部４１１により、ハッシュ値４１２３１がプログラム本体４１２１および公開鍵４１２２１と対をなす秘密鍵とによって生成されたものであるかどうかを確認する（ステップＳ４０１）。詳しくは、組み込み機能部４１１は、ハッシュ値４１２３１を公開鍵４１２２１で復号してプログラム本体４１２１をハッシングしたダイジェストを得る一方、プログラム本体４１２１を既知のハッシュ関数

でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値４１２３１がプログラム本体４１２１および公開鍵４１２２１と対をなす秘密鍵とによって生成されたものであるかどうかを確認する。すなわち、プログラム本体４１２１および公開鍵４１２２１が改竄されたものでなく、プログラム４１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器４１にプログラム４１２が導入、たとえばダウンロードされたときに１回行われればよい。

【０１２６】次に、携帯機器４１内のプログラム４１２を実行するプロセス４１２０が親機器４２と通信をしようとして通信要求を発生させた場合（ステップＳ４０２）、またはそれ以前に、親機器４２は、携帯機器４１に付随する公開鍵４１３２および秘密鍵４１３１を用いた公開鍵方式により携帯機器４１の認証を行う（ステップＳ４０３）。

【０１２７】たとえば、親機器４２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器４１に付随する公開鍵４１３２と、携帯機器４１が保持する携帯機器４１に付随する公開鍵４１３２とが一致するかどうかを判定し、一致した場合に携帯機器４１を認証する。

【０１２８】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器４２は携帯機器４１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器４１の組み込み機能部４１１はその文字列を携帯機器４１に付随する秘密鍵４１３１で暗号化して親機器４２に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器４２は暗号化した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器４１に付随する公開鍵４１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器４１を通信してよい相手（つまり、通信してよい相手を示す公開鍵として保持する携帯機器４１に付随する公開鍵４１３２と対をなす秘密鍵４１３１を所有するもの）であると認証する。

【０１２９】携帯機器４１の認証に成功した場合、親機器４２は、携帯機器４１の組み込み機能部４１１から公開鍵４１２２１を得、携帯機器４１によるハッシュ値確認結果に基づいてプログラム４１２が真正な出所由来をもつものであるかどうかを判定し（ステップＳ４０４）、そうであれば以降の通信によって発生する処理を公開鍵４１２２１に対応するユーザ権限でアクセス制御して実行する（ステップＳ４０５）。

【０１３０】一方、携帯機器４１の認証に失敗した場合（ステップＳ４０３）、プログラム４１２が真正な出所由来をもつものでなかった場合（ステップＳ４０４）、または公開鍵４１２２１に対応するユーザ権限が存在しない場合、親機器４２は、通信によって発生する処理を実行しないか、特定の決められたユーザ権限でアクセス制御して実行する（ステップＳ４０６）。

【０１３１】第４の実施の形態によれば、プログラム４１２が秘密鍵をもたなくても、親機器４２は、親機器４２と通信をしようとしてきた携帯機器４１内のプロセス４１２０の元となるプログラム４１２の認証が可能であることから、盗み見や改竄が可能な環境下にあるプログラム４１２を元にして動作する携帯機器４１と通信を行う場合に、親機器４２がプログラム４１２の成りすましを防止しかつ認証を行うことができる。

【０１３２】（５）　第５の実施の形態

図９を参照すると、本発明の第５の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器５１と、通信機能を有する通信・処理装置が適用された親機器５２と、携帯機器５１にインストールされ実行されるプログラム５１２とから、その主要部が構成されている。

【０１３３】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１３４】携帯機器５１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１３５】親機器５２としては、ＰＯＳ端末等が想定される。

【０１３６】携帯機器５１と親機器５２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１３７】携帯機器５１は、信頼できる組み込み機能部５１１と、プログラム５１２を実行するプロセス５１２０と、携帯機器５１に付随する秘密鍵５１３１および公開鍵５１３２とを含んで構成されている。

【０１３８】プログラム５１２は、プログラム本体５１２１と、プログラム５１２の出所由来を表す公開鍵群５１２２１～５１２２ｎと、プログラム本体５１２１および公開鍵群５１２２１～５１２２ｎを組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵５１２２１～５１２２ｎと対をなす各秘密鍵（図示せず）でそれぞれ暗号化した署名群であるハッシュ値群５１２３１～５１２３ｎとを含んで構成されている。なお、プログラム５１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体５１２１，公開鍵群５１２２１～５１２２ｎ，およびハッシュ値群５１２３１～５１２３ｎが一体として作成されている。

【０１３９】親機器５２は、通信してよい相手を示す公開鍵として、携帯機器５１に付随する公開鍵５１３２をもつ。

【０１４０】図１０を参照すると、携帯機器５１の組み込み機能部５１１および親機器５２の処理は、ハッシュ値確認ステップＳ５０１と、通信要求発生ステップＳ５

０２と、携帯機器認証ステップＳ５０３と、プログラム出所由来判定ステップＳ５０４と、通信・処理ステップＳ５０５と、通信・処理なしステップＳ５０６とからなる。

【０１４１】次に、このように構成された第５の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの動作について、図９および図１０を参照して詳細に説明する。

【０１４２】まず、携帯機器５１は、組み込み機能部５１１により、各ハッシュ値５１２３１～５１２３ｎがプログラム本体５１２１および公開鍵群５１２２１～５１２２ｎと各公開鍵５１２２１～５１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップＳ５０１）。詳しくは、組み込み機能部５１１は、各ハッシュ値５１２３１～５１２３ｎを各公開鍵５１２２１～５１２２ｎでそれぞれ復号してプログラム本体５１２１および公開鍵群５１２２１～５１２２ｎを組み合わせて作成されたデータをハッシングしたダイジェスト群を得る一方、プログラム本体５１２１および公開鍵群５１２２１～５１２２ｎを組み合わせて作成されたデータを既知のハッシュ関数でハッシングしてダイジェストを得、該ダイジェストとダイジェスト群の一つ一つとが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値５１２３１～５１２３ｎがプログラム本体５１２１および公開鍵群５１２２１～５１２２ｎと各公開鍵５１２２１～５１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体５１２１および公開鍵群５１２２１～５１２２ｎが、改竄されたものでなく、プログラム５１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器５１にプログラム５１２が導入、たとえばダウンロードされたときに１回行われればよい。

【０１４３】次に、携帯機器５１内のプログラム５１２を実行するプロセス５１２０が親機器５２と通信をしようとして通信要求が発生した場合(ステップＳ５０２)、またはそれ以前に、親機器５２は、携帯機器５１に付随する公開鍵５１３２および秘密鍵５１３１を用いた公開鍵方式により携帯機器５１の認証を行う（ステップＳ５０３）。

【０１４４】たとえば、親機器５２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器５１に付随する公開鍵５１３２と、携帯機器５１が保持する携帯機器５１に付随する公開鍵５１３２とが一致するかどうかを判定し、一致した場合に携帯機器５１の認証を行う。

【０１４５】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器５２は携帯機器５１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器５１の組み込み機能部５１１はその文字列を携帯機器５１に付随する秘密鍵５１３１で暗号化して親機器５２に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器５２は暗号化した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器５１に付随する公開鍵５１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器５１を通信してよい相手（つまり、通信してよい相手を示す公開鍵として保持する携帯機器５１に付随する公開鍵５１３２と対をなす秘密鍵５１３１を所有するもの）であると認証する。

【０１４６】携帯機器５１の認証に成功した場合、親機器５２は、携帯機器５１の組み込み機能部５１１からハッシュ値確認結果の公開鍵の集まりを得、携帯機器５１によるハッシュ値確認結果の公開鍵の集まりに１つ以上の公開鍵が含まれていればプログラム５１２が真正な出所由来をもつものであると判定し（ステップＳ５０４）、以降の通信によって発生する処理をハッシュ値確認結果の公開鍵の集まりの各公開鍵に対応するユーザ権限の組み合わせでアクセス制御して実行する（ステップＳ５０５）。

【０１４７】一方、携帯機器５１の認証に失敗した場合（ステップＳ５０３）、プログラム５１２が真正な出所由来をもつものでない場合（ステップＳ５０４）、または携帯機器５１によるハッシュ値確認結果の公開鍵の集まり中の公開鍵に対応するユーザ権限が１つも存在しない場合、親機器５２は、通信によって発生する処理を実行しないか、特定の制限されたユーザ権限でアクセス制御して実行する（ステップＳ５０６）。

【０１４８】なお、上記第５の実施の形態では、ステップＳ５０４で携帯機器５１によるハッシュ値確認結果の公開鍵の集まりに１つ以上の公開鍵が含まれていればプログラム５１２が真正な出所由来をもつものであると判定したが、携帯機器５１によるハッシュ値確認結果の公開鍵の集まりに公開鍵群５１２２１～５１２２ｎのすべてが含まれていたときにのみプログラム５１２が真正な出所由来をもつものであると判定するようにすることもできる。

【０１４９】第５の実施の形態によれば、プログラム５１２が該プログラム５１２の出所由来を表す公開鍵群５１２２１～５１２２ｎをもつことを許す場合はプログラム本体５１２１とともに保持する公開鍵群５１２２１～５１２２ｎに対して署名群であるハッシュ値群５１２３１～５１２３ｎを付すことから、プログラム５１２の成りすましを防止することができ、通信によって発生する処理をハッシュ値確認結果の公開鍵の集まりの各公開鍵に対応するユーザ権限の組み合わせでアクセス制御して実行することができる。

【０１５０】（６）　第６の実施の形態

図１１を参照すると、本発明の第６の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムは、プログラムの実行機能および通信機能を有する携帯機器６１と、同じくプログラムの実行機能および通信機能を有する親機器６２と、携帯機器６１にインストールされ実行されるプログラム６１２と、親機器６２にインストールされ実行されるプログラム６２２とから、その主要部が構成されている。

【０１５１】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１５２】携帯機器６１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１５３】親機器６２としては、ＰＯＳ端末等が想定される。

【０１５４】携帯機器６１と親機器６２との間の通信機能に使用される通信方式は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１５５】携帯機器６１は、信頼できる組み込み機能部６１１と、プログラム６１２を実行するプロセス６１２０とを含んで構成されている。

【０１５６】プログラム６１２は、プログラム本体６１２１と、プログラム６１２の出所由来を表す公開鍵６１２２および秘密鍵６１２４とを含んで構成されている。なお、プログラム６１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体６１２１，公開鍵６１２２および秘密鍵６１２４が一体として作成されている。

【０１５７】親機器６２は、信頼できる組み込み機能部６２１と、プログラム６２２を実行するプロセス６２２０とを含んで構成されている。

【０１５８】プログラム６２２は、プログラム本体６２２１と、プログラム６２２の出所由来を表す公開鍵６２２２および秘密鍵６２２４とを含んで構成されている。なお、プログラム６２２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体６２２１，公開鍵６２２２および秘密鍵６２２４が一体として作成されている。

【０１５９】図１２を参照すると、携帯機器６１の組み込み機能部６１１および親機器６２の組み込み機能部６２１の処理は、通信要求発生ステップＳ６０１と、公開鍵獲得ステップＳ６０２と、相互認証ステップＳ６０３と、公開鍵比較ステップＳ６０４と、相互認証・公開鍵一致判定ステップＳ６０５と、通信許可ステップＳ６０６と、通信不許可ステップＳ６０７とからなる。

【０１６０】次に、このように構成された第６の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの動作について、図１１および図１２を参照して詳細に説明する。

【０１６１】携帯機器６１内のプログラム６１２を実行するプロセス６１２０と親機器６２内のプログラム６２２を実行するプロセス６２２０との間で通信要求が発生した場合（ステップＳ６０１），まず、携帯機器６１の組み込み機能部６１１は、親機器６２の組み込み機能部６２１にプロセス６１２０の元となるプログラム６１２の出所由来を表す公開鍵６１２２を送り、親機器６２の組み込み機能部６２１は、携帯機器６１の組み込み機能部６１１にプロセス６２２０の元となるプログラム６２２の出所由来を表す公開鍵６２２２を送り(ステップＳ６０２)、次に、双方で、公開鍵６１２２と公開鍵６２２２とが一致するかどうかを調べる(ステップＳ６０３)。

【０１６２】次に、携帯機器６１の組み込み機能部６１１と親機器６２の組み込み機能部６２１との間で、プログラム６１２およびプログラム６２２の相互認証を行う（ステップＳ６０４）。

【０１６３】たとえば、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、携帯機器６１の組み込み機能部６１１は親機器６２の組み込み機能部６２１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、親機器６２の組み込み機能部６２１はその文字列をプログラム６２２の秘密鍵６２２４で暗号化して携帯機器６１の組み込み機能部６１１に送り返し（”Ｒｅｓｐｏｎｓｅ”）、携帯機器６１の組み込み機能部６１１は、暗号化した文字列を公開鍵６２２２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、プロセス６２２０の元となるプログラム６２２が公開鍵６２２２をもつ（つまり、プロセス６２２０の元となるプログラム６２２が公開鍵６２２２と対をなす秘密鍵６２２４をもつ）と認証する。

【０１６４】一方、親機器６２の組み込み機能部６２１は携帯機器６１の組み込み機能部６１１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”），携帯機器６１の組み込み機能部６１１はその文字列を携帯機器６１に付随する秘密鍵６１２４で暗号化して親機器６２の組み込み機能部６２１に送り返し（”Ｒｅｓｐｏｎｓｅ”），親機器６２の組み込み機能部６２１は、暗号化した文字列を公開鍵６１２２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、プロセス６１２０の元となるプログラム６１２が公開鍵６１２２をもつ（つまり、プロセス６１２０の元となるプログラム６１２が公開鍵６１２２と対をなす秘密鍵６１２４をもつ）と認証する。

【０１６５】プログラム６１１およびプログラム６１２の相互認証が成功し、かつ公開鍵６１２２と公開鍵６２２２とが一致した場合（ステップＳ６０５），携帯機器６１の組み込み機能部６１１および親機器６２の組み込み機能部６２１は、プロセス６１２１０とプロセス６２２１０との間で通信を許可する（ステップＳ６０６）。

【０１６６】逆に、プログラム６１１およびプログラム

６１２の相互認証に失敗した場合、あるいはプログラム６１２の出所由来を表す公開鍵６１２２とプログラム６２２の出所由来を表す公開鍵６２２２とが一致しなかった場合、携帯機器６１の組み込み機能部６１１および親機器６２の組み込み機能部６２１は、プロセス６１２０とプロセス６２２０との間で通信を不許可とする（ステップＳ６０７）。

【０１６７】第６の実施の形態によれば、携帯機器６１内のプログラム６１２および親機器６２内のプログラム６２２が、一致する公開鍵６１２２および６２２２を付随するプログラム６１２および６２２としか通信できず、任意の他のプログラムと通信できないため、携帯機器６１内のプログラム６１２および親機器６２内のプログラム６２２のもつ情報の、流通する範囲を出所由来を同じくするプログラムの範囲内に限ることができる。

【０１６８】また、携帯機器６１内のプログラム６１２および親機器６２内のプログラム６２２が、一致する公開鍵６１２２および６２２２を付随するプログラム６１２および６２２としか通信できず、任意の他のプログラムと通信できないため、携帯機器６１内のプログラム６１２および親機器６２内のプログラム６２２のもつ情報が、たとえプログラム６１２および６２２が暴走しても、出所由来を同じくするプログラムの範囲外に漏洩しない。

【０１６９】さらに、分散環境における通信範囲の制御についてのセキュリティ面での設計が容易になり、かつ自由度が変わらないことである。その理由は、分散環境におけるもっとも重要な問題の１つである通信時の情報漏洩について、製造元またはそれに類するものを同じくするプログラムの間でしか情報を流通させないために、設計時に情報の流通範囲を設計しなくても、悪意のある他者への漏洩や、プログラムのバグ，暴走による漏洩が起こらず、また、逆に１つのサービスにおいては、そのプロジェクトにかかわるもの全体である１つの製造元またはそれに類するものとみなすことで、情報の流通を行え、またその流通範囲で十分であるからである。

【０１７０】（７）　第７の実施の形態

図１３を参照すると、本発明の第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムは、プログラムの実行機能および通信機能を有する携帯機器７１と、同じくプログラムの実行機能および通信機能を有する親機器７２と、携帯機器７１にインストールされ実行されるプログラム７１２と、親機器７２にインストールされ実行されるプログラム７２２とから、その主要部が構成されている。

【０１７１】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１７２】携帯機器７１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１７３】親機器７２としては、ＰＯＳ端末等が想定される。

【０１７４】携帯機器７１と親機器７２との間の通信機能に使用される通信方式は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１７５】携帯機器７１は、信頼できる組み込み機能部７１１と、プログラム７１２を実行するプロセス７１２０と、携帯機器７１に付随する秘密鍵７１３１および公開鍵７１３２と、親機器７２に付随する公開鍵７２３２とを含んで構成されている。

【０１７６】プログラム７１２は、プログラム本体７１２１と、プログラム７１２の出所由来を表す公開鍵７１２２と、プログラム本体７１２１をハッシュ関数でハッシングしたダイジェストを公開鍵７１２２と対をなす秘密鍵（図示せず）で暗号化した署名であるハッシュ値７１２３とを含んで構成されている。なお、プログラム７１２は、その出所（製造元等）および由来（バージョン等）においてプログラム本体７１２１，公開鍵７１２２，およびハッシュ値７１２３が一体として作成されている。

【０１７７】親機器７２は、信頼できる組み込み機能部７２１と、プログラム７２２を実行するプロセス７２２０と、親機器７２に付随する秘密鍵７２３１および公開鍵７２３２と、携帯機器７１に付随する公開鍵７１３２とを含んで構成されている。

【０１７８】プログラム７２２は、プログラム本体７２２１と、プログラム７２２の出所由来を表す公開鍵７２２２と、プログラム本体７２２１をハッシュ関数でハッシングしたダイジェストを公開鍵７２２２と対をなす秘密鍵（図示せず）で暗号化した署名であるハッシュ値７２２３とを含んで構成されている。なお、プログラム７２２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体７２２１，公開鍵７２２２，およびハッシュ値７２２３が一体として作成されている。

【０１７９】図１４を参照すると、携帯機器７１の組み込み機能部７１１および親機器７２の組み込み機能部７２１の処理は、ハッシュ値確認ステップＳ７０１およびＳ７０２と、通信要求発生ステップＳ７０３と、相互認証ステップＳ７０４と、公開鍵一致判定ステップＳ７０５と、通信許可ステップＳ７０６と、通信不許可ステップＳ７０７とからなる。

【０１８０】次に、このように構成された第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの動作について、図１３および図１４を参照して詳細に説明する。

【０１８１】まず、携帯機器７１は、組み込み機能部７１１により、ハッシュ値７１２３がプログラム本体７１２１および公開鍵群７１２２と公開鍵７１２２と対をなす秘密鍵とによって生成されたものであるかどうかを確

認する（ステップＳ７０１）。詳しくは、組み込み機能部７１１は、ハッシュ値７１２３を公開鍵７１２２で復号してプログラム本体７２２１をハッシングしたダイジェストを得る一方、プログラム本体７１２１を既知のハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値７１２３がプログラム本体７１２１および公開鍵群７１２２と公開鍵７１２２と対をなす秘密鍵とによって生成されたものであるかどうかを確認する。すなわち、プログラム本体７１２１および公開鍵７１２２が改竄されたものでなく、プログラム７１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器７１にプログラム７１２が導入、たとえばダウンロードされたときなどに１回行われればよい。

【０１８２】また、親機器７２も、組み込み機能部７２１により、ハッシュ値７２２３がプログラム本体７２２１および公開鍵群７２２２と公開鍵７２２２と対をなす秘密鍵とによって生成されたものであるかどうかを確認する（ステップＳ７０２）。詳しくは、組み込み機能部７２１は、ハッシュ値７２２３を公開鍵７２２２で復号してプログラム本体７２２１をハッシングしたダイジェストを得る一方、プログラム本体７２２１を既知のハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値７２２３がプログラム本体７２２１および公開鍵群７２２２と公開鍵７２２２と対をなす秘密鍵とによって生成されたものであることを確認する。すなわち、プログラム本体７２２１および公開鍵７２２２が改竄されたものでなく、プログラム７２２が真正な出所由来をもつことを確認する。なお、この確認処理は、親機器７２にプログラム７２２が導入、たとえばインストールされたときなどに１回行われればよい。

【０１８３】次に、携帯機器７１内のプログラム７１２を実行するプロセス７１２０と親機器７２内のプログラム７２２を実行するプロセス７２２０とが通信をしようとして通信要求が発生した場合（ステップＳ７０３）、またはそれ以前に、まず、携帯機器７１の組み込み機能部７１１と親機器７２の組み込み機能部７２１との間で、携帯機器７１が付随する秘密鍵７１３１および公開鍵７１３２と、親機器７２に付随する秘密鍵７２３１および公開鍵７２３２とを用いた公開鍵方式により携帯機器７１および親機器７２の相互認証を行う（ステップＳ７０４）。

【０１８４】たとえば、親機器７２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器７１に付随する公開鍵７１３２と、携帯機器７１が保持する携帯機器７１に付随する公開鍵７１１３２とが一致するかどうかを判定し、一致した場合に携帯機器７１の認証を行う。一方、携帯機器７１は、自らが通信してよい相手を示す公開鍵として保持する親機器７２に付随する公開鍵７２３２と、親機器７２が保持する親機器７２に付随する公開鍵７２１３２とが一致するかどうかを判定し、一致した場合に親機器７２の認証を行う。

【０１８５】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、携帯機器７１の組み込み機能部７１１は親機器７２にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、親機器７２の組み込み機能部７２１はその文字列を親機器７２に付随する秘密鍵７２３１で暗号化して携帯機器７１に送り返し（”Ｒｅｓｐｏｎｓｅ”）、携帯機器７１の組み込み機能部７１１は、暗号化した文字列を親機器７２に付随する公開鍵７２３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、親機器７２を通信してよい相手（つまり、親機器７２に付随する公開鍵７２３２と対をなす秘密鍵７２３１を所有するもの）であると認証する。一方、親機器７２の組み込み機能部７２１は携帯機器７１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器７１の組み込み機能部７１１はその文字列を携帯機器７１に付随する秘密鍵７１３１で暗号化して親機器７２に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器７２の組み込み機能部７２１は暗号化した文字列を携帯機器７１に付随する公開鍵７１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば携帯機器７１を通信してよい相手（つまり、携帯機器７１に付随する公開鍵７１３２と対をなす秘密鍵７１３１を所有するもの）であると認証する。

【０１８６】相互認証に成功した場合、携帯機器７１の組み込み機能部７１１および親機器７２の組み込み機能部７２１は、プログラム７１２の出所由来を表す公開鍵７１２２とプログラム７２２の出所由来を表す公開鍵７２２２とをお互いに相手に伝え、両公開鍵が一致するかどうかを判定し（ステップＳ７０５）、一致した場合に限り、プロセス７１２１０とプロセス７２２１０との間で通信を許可する（ステップＳ７０６）。

【０１８７】携帯機器７１と親機７２との相互認証に失敗した場合（ステップＳ７０４）、またはプログラム７１２の出所由来を表す公開鍵７１２２とプログラム７２２の出所由来を表す公開鍵７２２２とが一致しなかった場合（ステップＳ７０５）、携帯機器７１の組み込み機能部７１１および親機器７２の組み込み機能部７２１は、プロセス７１２０とプロセス７２２０との間の通信を不許可とする（ステップＳ７０７）。

【０１８８】第７の実施の形態によれば、携帯機器７１内のプログラム７１２および親機器７２内のプログラム７２２が、一致する公開鍵７１２２および７２２２を付随するプログラム７１２および７２２としか通信できず、任意の他のプログラムと通信できないため、携帯機器７１内のプログラム７１２および親機器７２内のプログラム７２２のもつ情報の、流通する範囲を出所由来を同じくするプログラムの範囲内に限ることができる。

【０１８９】また、携帯機器７１内のプログラム７１２および親機器７２内のプログラム７２２が、一致する公開鍵７１２２および７２２２を付随するプログラム７１２および７２２としか通信できず、任意の他のプログラムと通信できないため、携帯機器７１内のプログラム７１２および親機器７２内のプログラム７２２のもつ情報が、たとえプログラム７１２および７２２が暴走しても、出所由来を同じくするプログラムの範囲外に漏洩しない。

【０１９０】さらに、分散環境における通信範囲の制御についてのセキュリティ面での設計が容易になり、かつ自由度が変わらないことである。その理由は、分散環境におけるもっとも重要な問題の１つである通信時の情報漏洩について、製造元またはそれに類するものを同じくするプログラムの間でしか情報を流通させないために、設計時に情報の流通範囲を設計しなくても、悪意のある他者への漏洩や、プログラムのバグ，暴走による漏洩が起こらず、また、逆に１つのサービスにおいては、そのプロジェクトにかかわるもの全体である１つの製造元またはそれに類するものとみなすことで、情報の流通を行え、またその流通範囲で十分であるからである。

【０１９１】さらに、プログラム７１２、７２２が秘密鍵をもたなくても、携帯機器７１および親機７２は、相手内のプロセス７２２０、７１２０、の元となるプログラム７２２、７１２の認証が可能であることから、盗み見や改竄が可能な環境下にあるプログラム７１２、７２２を元にして動作する相手と通信を行う場合に、携帯機器７１、親機器７２がプログラム７２２、７１２の成りすましを防止しかつ認証を行うことができる。

【０１９２】（８）　第８の実施の形態

図１５を参照すると、本発明の第８の実施の形態に係るプログラムＩＤ通信範囲制御方法および公開鍵毎通信路提供方法が適用された情報システムは、第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムにおいて、携帯機器８１および親機器８２が、さらに、通信装置８１５および８２５と、公開鍵毎にすべてのポート番号を割り振ることの出来る、つまり同じポート番号で公開鍵値毎に存在し得る仮想ソケット８１５１１～８１５１ｉおよび８２６１１～８２５１ｊと、ソケット８１５２１～８１５２ｋおよび８２５２１～８２５２１とを含んで構成されている。なお、第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムにおける部分と対応する部分には、符号の先頭文字「７」を「８」に変更した符号を付して、それらの詳しい説明を省略する。

【０１９３】仮想ソケット８１５１１～８１５１ｉおよび８２６１１～８２５１ｊは、チャネル，パイプ等の他の通信路を仮想的にしたものでもよく、ソケット８１５２１～８１５２ｋおよび８２５２１～８２５２１、チャネル，パイプ等の他の通信路であってもよい。

【０１９４】図１６を参照すると、携帯機器８１の組み込み機能部８１１および親機器８２の組み込み機能部８２１の処理は、ハッシュ値確認ステップＳ８０１およびＳ８０２と、通信要求発生ステップＳ８０３と、相互認証ステップＳ８０４と、公開鍵一致判定ステップＳ８０５と、通信許可ステップＳ８０６と、通信不許可ステップＳ８０７とからなる。

【０１９５】次に、このように構成された第８の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの動作について、図１５および図１６を参照して詳細に説明する。

【０１９６】ステップＳ８０１～ステップＳ８０５およびステップＳ８０７は、第７の実施の形態に係るプログラムＩＤ通信範囲制御方法におけるステップＳ７０１～ステップＳ７０５およびステップＳ７０７と同じである。

【０１９７】第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの動作において、プロセス８１２０とプロセス８２２０との間で通信を許可するステップＳ８０６において、一致した場合に限り、通信装置８１５および８２５は、それぞれ、公開鍵８１２２および８２２２とプロセス８１２１０およびプロセス８２２１０が要求する仮想ソケットのポート番号の対に対し、組み込み機能部８１１と組み込み機能部８２１との間で使用しているソケットによる通信路に形成された仮想通信路の１つを割り当て、該仮想通信路によりプロセス８１２１０とプロセス８２２１０との間での通信を許可する。

【０１９８】（９）　第９の実施の形態

図１７を参照すると、本発明の第９の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムは、プログラムの実行機能および通信機能を有する携帯機器９１と、同じくプログラムの実行機能および通信機能を有する親機器９２と、携帯機器９１にインストールされ実行されるプログラム９１２と、親機器９２にインストールされ実行されるプログラム９２２とから、その主要部が構成されている。

【０１９９】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０２００】携帯機器９１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０２０１】親機器９２としては、ＰＯＳ端末等が想定される。

【０２０２】携帯機器９１と親機器９２との間の通信機能に使用される通信方式は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０２０３】携帯機器９１は、信頼できる組み込み機能部９１１と、プログラム９１２を実行するプロセス９１２０と、携帯機器９１に付随する秘密鍵９１３１および

公開鍵９１３２と、親機器９２に付随する公開鍵９２３２とを含んで構成されている。

【０２０４】プログラム９１２は、プログラム本体９１２１と、プログラム９１２の出所由来を表す公開鍵群９１２２１～９１２２ｎと、プログラム本体９１２１および公開鍵群９１２２１～９１２２ｎを組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵９１２２１～９１２２ｎと対をなす各秘密鍵（図示せず）で暗号化した署名群であるハッシュ値群９１２３１～９１２３ｎとを含んで構成されている。なお、プログラム９１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体９１２１，公開鍵群９１２２１～９１２２ｎ，およびハッシュ値群９１２３１～９１２３ｎが一体として作成されている。

【０２０５】親機器９２は、信頼できる組み込み機能部９２１と、プログラム９２２を実行するプロセス９２２０と、親機器９２に付随する秘密鍵９２３１および公開鍵９２３２と、携帯機器９１に付随する公開鍵９１３２とを含んで構成されている。

【０２０６】プログラム９２２は、プログラム本体９２２１と、プログラム９２２の出所由来を表す公開鍵群９２２２１～９２２２ｍ（ｍは２上の正整数。以下同様）と、プログラム本体９２２１および公開鍵群９２２２１～９２２２ｍにより構成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵９２２２１～９２２２ｍと対をなす各秘密鍵（図示せず）で暗号化した署名群であるハッシュ値群９２２３１～９２２３ｍとを含んで構成されている。なお、プログラム９２２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体９２２１，公開鍵群９２２２１～９２２２ｍ，およびハッシュ値群９２２３１～９２２３ｍが一体として作成されている。

【０２０７】図１８を参照すると、携帯機器９１の組み込み機能部９１１および親機器９２の組み込み機能部９２１の処理は、ハッシュ値確認ステップＳ９０１およびＳ９０２と、通信要求発生ステップＳ９０３と、相互認証ステップＳ９０４と、公開鍵一致判定ステップＳ９０５と、通信許可ステップＳ９０６と、通信不許可ステップＳ９０７とからなる。

【０２０８】次に、このように構成された第９の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの動作について、図１７および図１８を参照して詳細に説明する。

【０２０９】まず、携帯機器９１は、組み込み機能部９１１により、各ハッシュ値９１２３１～９１２３ｎがプログラム本体９１２１および公開鍵群９１２２１～９１２２ｎと各公開鍵９１２２１～９１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップＳ９０１）。詳しくは、組み込み機能部９１１は、各ハッシュ値９１２３１～９１２３ｎを各公開鍵９１２２１～９１２２ｎでそれぞれ復号してプログラム本体９１２１および公開鍵群９１２２１～９１２２ｎを組み合わせて作成されたデータをハッシングしたダイジェスト群を得る一方、プログラム本体９１２１および公開鍵群９１２２１～９１２２ｎを組み合わせて作成されたデータを既知のハッシュ関数でハッシングしてダイジェストを得、該ダイジェストとダイジェスト群の一つ一つが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値９１２３１～９１２３ｎがプログラム本体９１２１および公開鍵群９１２２１～９１２２ｎと各公開鍵９１２２１～９１２２ｎと対をなす各秘密鍵とによって生成されたものであることをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体９１２１および公開鍵群９１２２１～９１２２ｎ中の少なくとも１つ以上の公開鍵が改竄されたものでなく、真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器９１にプログラム９１２が導入、たとえばダウンロードされたときなどに１回行われればよい。

【０２１０】また、携帯機器９２でも、組み込み機能部９２１が、各ハッシュ値９２２３１～９２２３ｎがプログラム本体９２２１および公開鍵群９２２２１～９２２２ｎと各公開鍵９２２２１～９２２２ｎと対をなす各秘密鍵（図示せず）とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップＳ９０２）。詳しくは、組み込み機能部９２１は、各ハッシュ値９２２３１～９２２３ｍを公開鍵９２２２１～９２２２ｍでそれぞれ復号してプログラム本体９２２１および公開鍵群９２２２１～９２２２ｍを組み合わせて作成されたデータをハッシングした各ダイジェストを得る一方、プログラム本体９２２１および公開鍵群９２２２１～９２２２ｍを組み合わせて作成されたデータを既知のハッシュ関数でハッシングしたダイジェストを得、両各ダイジェストが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値９２２３１～９２２３ｎがプログラム本体９２２１および公開鍵群９２２２１～９２２２ｎと各公開鍵９２２２１～９２２２ｎと対をなす各秘密鍵（図示せず）とによって生成されたものであることをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体９２２１および公開鍵群９２２２１～９２２２ｍ中の少なくとも１つ以上の公開鍵が改竄されたものでなく、真正な出所由来をもつことを確認する。なお、この確認処理は、親機器９２にプログラム９２２が導入、たとえばインストールされたときなどに１回行われればよい。

【０２１１】次に、携帯機器９１内のプログラム９１２を実行するプロセス９１２０と親機器９２内のプログラ

ム９２２を実行するプロセス９２２０とが通信をしようとして通信要求が発生した場合（ステップＳ９０３）、またはそれ以前に、まず、携帯機器９１の組み込み機能部９１１と親機器９２の組み込み機能部９２１との間で、携帯機器９１に付随する秘密鍵９１３１および公開鍵９１３２と、親機器９２に付随する秘密鍵９２３１および公開鍵９２３２とを用いた公開鍵方式により相互認証を行う（ステップＳ９０４）。

【０２１２】たとえば、親機器９２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器９１に付随する公開鍵９１３２と、携帯機器９１が保持する携帯機器９１に付随する公開鍵９１１３２とが一致するかどうかを判定し、一致した場合に携帯機器９１の認証を行う。一方、携帯機器９１は、自らが通信してよい相手を示す公開鍵として保持する親機器９２に付随する公開鍵９２３２と、親機器９２が保持する親機器９２に付随する公開鍵９２１３２とが一致するかどうかを判定し、一致した場合に親機器９２の認証を行う。

【０２１３】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、携帯機器９１の組み込み機能部９１１は親機器９２にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、親機器９２の組み込み機能部９２１はその文字列を親機器９２に付随する秘密鍵９２３１で暗号化して携帯機器９１に送り返し（”Ｒｅｓｐｏｎｓｅ”）、携帯機器９１の組み込み機能部９１１は、暗号化した文字列を親機器９２に付随する公開鍵９２３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、親機器９２を通信してよい相手（つまり、親機器９２に付随する公開鍵９２３２と対をなす秘密鍵９２３１を所有するもの）であると認証する。一方、親機器９２の組み込み機能部９２１は携帯機器９１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器９１の組み込み機能部９１１はその文字列を携帯機器９１に付随する秘密鍵９１３１で暗号化して親機器９２に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器９２の組み込み機能部９２１は暗号化した文字列を携帯機器９１に付随する公開鍵９１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器９１を通信してよい相手（つまり、携帯機器９１に付随する公開鍵９１３２と対をなす秘密鍵９１３１を所有するもの）であると認証する。

【０２１４】相互認証に成功した場合、携帯機器９１の組み込み機能部９１１および親機器９２の組み込み機能部９２１は、ハッシュ値確認結果の公開鍵の集まりをお互いに相手に伝え、一致する公開鍵があるかどうかを判定し（ステップＳ９０５）、一致する公開鍵が１つ以上ある場合に限り、プロセス９１２１０とプロセス９２２１０との間で通信を許可する（ステップＳ９０６）。

【０２１５】ステップＳ９０４で携帯機器９１または親機９２の相互認証に失敗した場合、またはステップＳ９０５で一致する公開鍵が１つもなかった場合、携帯機器９１の組み込み機能部９１１および親機器９２の組み込み機能部９２１は、プロセス９１２０とプロセス９２２０との間の通信を不許可とする（ステップＳ９０７）。

【０２１６】なお、上記第９の実施の形態では、ステップＳ９０５で携帯機器９１によるハッシュ値確認結果の公開鍵の集まりと親機器９２によるハッシュ値確認結果の公開鍵の集まりとに一致する公開鍵が１つ以上含まれていればプログラム９１２および９２２が真正な出所由来をもつものであると判定したが、携帯機器９１によるハッシュ値確認結果の公開鍵の集まりと親機器９２によるハッシュ値確認結果の公開鍵の集まりとの公開鍵がすべて一致したときにのみ、プロセス９１２１０とプロセス９２２１０との間で通信を許可するようにすることもできる。

【０２１７】第９の実施の形態によれば、プログラム９１２および９２２が該プログラム９１２および９２２の出所由来を表す公開鍵群９１２２１～９１２２ｎおよび９２２２１～９２２２ｎをもつことを許す場合はプログラム本体９１２１および９２２１とともに保持する公開鍵群９１２２１～９１２２ｎおよび９２２２１～９２２２ｎに対して署名群であるハッシュ値群９１２３１～９１２３ｎおよび９２２３１～９２２３ｎを付すことから、プログラム５１２および５２２の成りすましを防止することができる。

【０２１８】

【発明の効果】第１の効果は、外部装置が、盗み見や改竄が可能な環境下にあるプログラムを元にし動作する装置と通信を行う場合に、成りすましを防止しかつ通信相手のプログラムの認証を行うことができることである。その理由は、プログラムが秘密鍵をもたないで認証が可能だからである。

【０２１９】第２の効果は、プログラムが成りすましを防止しかつ複数の出所由来を表す公開鍵をもつことを許すことができることである。その理由は、複数の出所由来を表す公開鍵をもつことを許す場合は、プログラム本体とともに保持する公開鍵群に対し署名するからである。

【０２２０】第３の効果は、悪意のプログラムに対しセキュリティを保てることである。その理由は、プログラムの出所由来を表すＩＤ、つまりプログラムの製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うからである。

【０２２１】第４の効果は、ユーザ管理のような集中管理システムを必要としない分散環境下での通信による処理についてのセキュリティを保てることである。その理由は、プログラムの出所由来を表すＩＤ、つまりプログラムの製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うため、悪意のプログラムに対しセキュリティを保てるからである。

【０２２２】第５の効果は、プログラム実行・通信装置内のプログラムのもつ情報の、流通する範囲が出所由来を同じくするプログラムの範囲内に限られることである。その理由は、プログラム実行・通信装置内のプログラムが、一致する出所由来を表すＩＤを有するプログラムとしか通信できず、任意の他のプログラムと通信できないためである。

【０２２３】第６の効果は、プログラム実行・通信装置内のプログラムのもつ情報が、たとえプログラムが暴走しても、出所由来を同じくするプログラムの範囲外に漏洩しないことである。その理由は、プログラム実行・通信装置内のプログラムが、一致する出所由来を表すＩＤを有するプログラムとしか通信できず、任意の他のプログラムと通信できないためである。

【０２２４】第７の効果は、プログラム実行・通信装置内のプログラムのもつ情報の、流通する範囲が、出所由来を同じくするプログラムの範囲内に限られることである。その理由は、プログラム実行・通信装置内のプログラムが、一致する出所由来を表すＩＤを公開鍵とすることにより、同じ秘密鍵を保持するものにより提供されたプログラムの間でしか、通信ができないからである。

【０２２５】第８の効果は、分散環境における通信範囲の制御についてのセキュリティ面での設計が容易になり、かつ自由度が変わらないことである。その理由は、分散環境におけるもっとも重要な問題の１つである通信時の情報漏洩について、出所由来を同じくするプログラムの間でしか情報を流通させないために、設計時に情報の流通範囲を設計しなくても、悪意のある他者への漏洩や、プログラムのバグ、暴走による漏洩が起こらず、また、逆に１つのサービスにおいては、そのプロジェクトにかかわるもの全体である１つの製造元またはそれに類するものとみなすことで、情報の流通を行え、またその流通範囲で十分であるからである。

【０２２６】第９の効果は、悪意のプログラムに対しセキュリティを保てることである。その理由は、プログラムの出所由来を表すＩＤ、つまりプログラムの製造元やバージョンに類する情報を元に通信可否を行うからである。

【０２２７】第１０の効果は、ユーザ管理のような集中管理システムを必要としない分散環境下での通信による処理についてのセキュリティを保てることである。その理由は、プログラムの出所由来を表すＩＤ、つまりプログラムの製造元やバージョンに類する情報を元に通信可否を行うため、悪意のプログラムに対しセキュリティを保てるからである。

【０２２８】第１１の効果は、公開鍵別の通信を行う場合に、通信路に関するシステム設計が容易であることである。その理由は、どの通信路がどの公開鍵用で占有されるかが予め限定されているからである。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの構成を示すブロック図である。

【図２】第１の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの処理を示す流れ図である。

【図３】本発明の第２の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの構成を示すブロック図である。

【図４】第２の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの処理を示す流れ図である。

【図５】本発明の第３の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの構成を示すブロック図である。

【図６】第３の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの処理を示す流れ図である。

【図７】本発明の第４の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの構成を示すブロック図である。

【図８】第４の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの処理を示す流れ図である。

【図９】本発明の第５の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの構成を示すブロック図である。

【図１０】第５の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの処理を示す流れ図である。

【図１１】本発明の第６の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの構成を示すブロック図である。

【図１２】第６の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

【図１３】本発明の第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの構成を示すブロック図である。

【図１４】第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

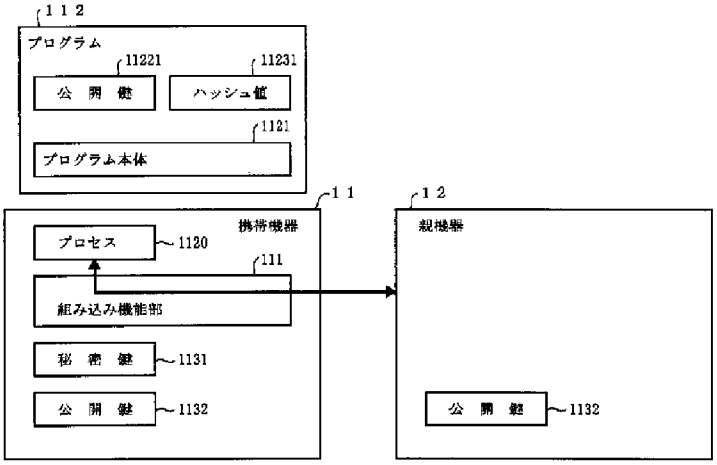
【図１５】本発明の第８の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの構成を示すブロック図である。

【図１６】第８の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

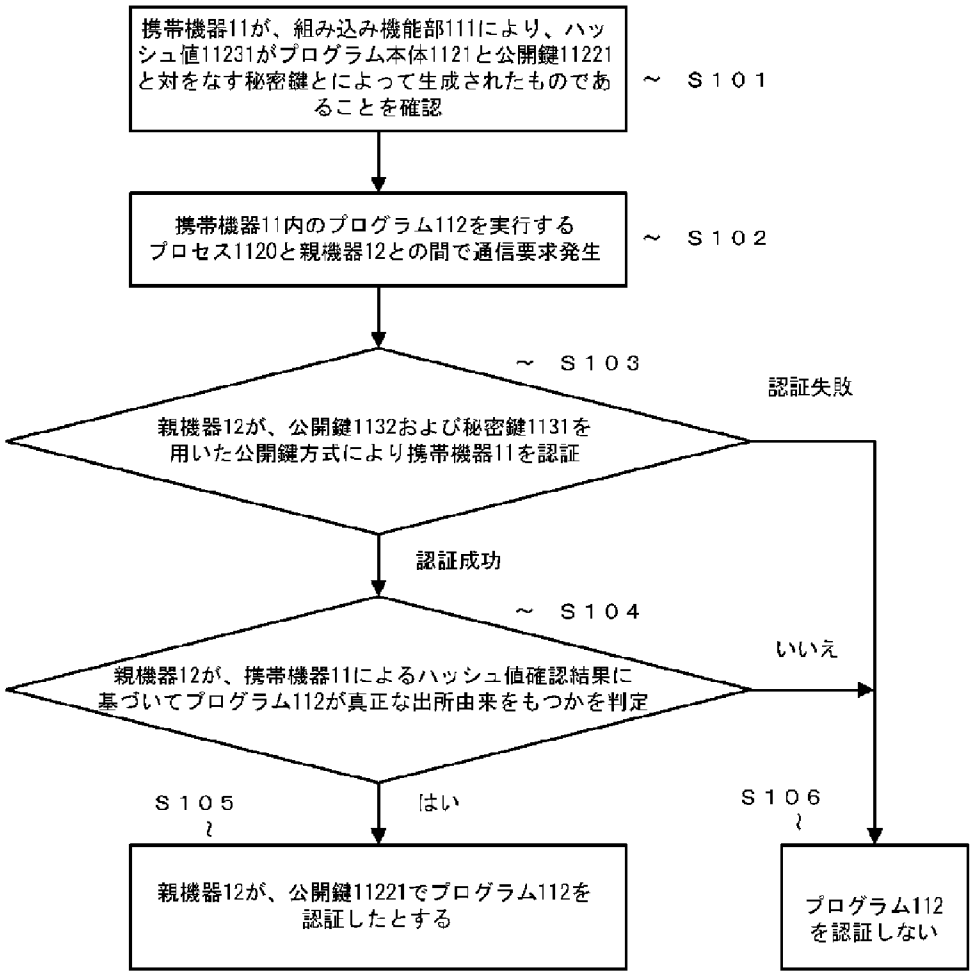
【図１７】本発明の第９の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの構成

を示すブロック図である。
【図１８】第９の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの処理を示す流れ図である。
【図１９】従来の情報システムの構成の一例を説明するブロック図である。
【図２０】従来の情報システムの構成の他の例を説明するブロック図である。
【図２１】従来の情報システムの構成の別の例を説明するブロック図である。
【符号の説明】
１１，…，９１　携帯機器
１２，…，９２　親機器
１１１，…，９１１　組み込み機能部
１１２，…，９１２　プログラム
１１２０，…，９１２０　プロセス
１１２１，…，９１２１　プログラム本体
１１２２１～１１２２ｎ，…，９１２２１～９１２２ｎ　公開鍵
１１２３１～１１２３ｎ，…，９１２３１～９１２３ｎ　ハッシュ値
１１２４１～１１２４ｎ，…，９１２４１～９１２４ｎ　秘密鍵
１１３１，…，９１３１　秘密鍵
１１３２，…，９１３２　公開鍵
８１５１１～８１５１ｉ，８２５１１～８２５１ｊ　仮想ソケット
８１５２１～８１５２ｋ，８２５２１～８２５２１　ソケット
Ｓ１０１，Ｓ２０１，Ｓ４０１，Ｓ５０１，Ｓ７０１，Ｓ７０２，Ｓ８０１，Ｓ８０２，Ｓ９０１，Ｓ９０２　ハッシュ値確認ステップ
Ｓ１０２，Ｓ２０２，Ｓ３０１，Ｓ４０２，Ｓ５０２，Ｓ６０１，Ｓ７０３，Ｓ８０３，Ｓ９０３　通信要求発生ステップ
Ｓ１０３，Ｓ２０３，Ｓ４０３，Ｓ５０３　携帯機器認証ステップ
Ｓ１０４，Ｓ２０４，Ｓ４０４，Ｓ５０４　プログラム出所由来判定ステップ
Ｓ１０５，Ｓ２０５，Ｓ３０３　プログラム認証ステップ
Ｓ１０６，Ｓ２０６　プログラム不認証ステップ
Ｓ３０２，Ｓ６０２　公開鍵獲得ステップ
Ｓ３０４，Ｓ４０５，Ｓ５０５　通信・処理ステップ
Ｓ３０５，Ｓ４０６，Ｓ５０６　通信・処理なしステップ
Ｓ６０３，Ｓ７０４　相互認証ステップ
Ｓ６０４　公開鍵比較ステップ
Ｓ６０５　相互認証・公開鍵一致判定ステップ
Ｓ６０６，Ｓ７０６，Ｓ８０６，Ｓ９０６　通信許可ステップ
Ｓ６０７，Ｓ７０７，Ｓ８０７，Ｓ９０７　通信不許可ステップ
Ｓ７０５，Ｓ８０５，Ｓ９０５　公開鍵一致判定ステップ
Ｓ８０４，Ｓ９０４　相互認証ステップ

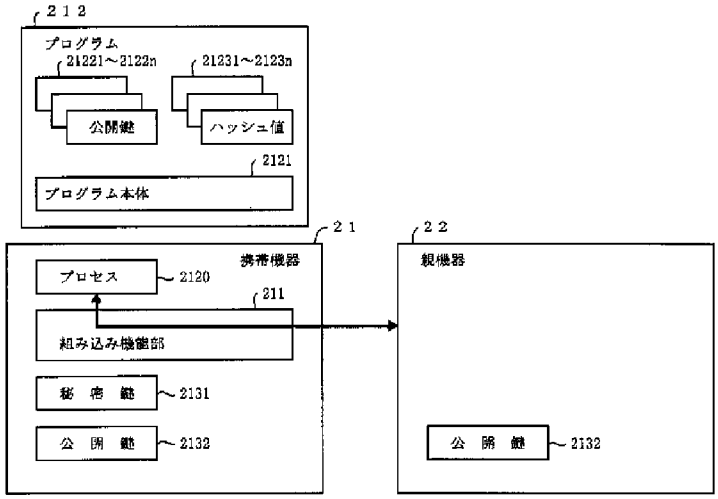
【図１】



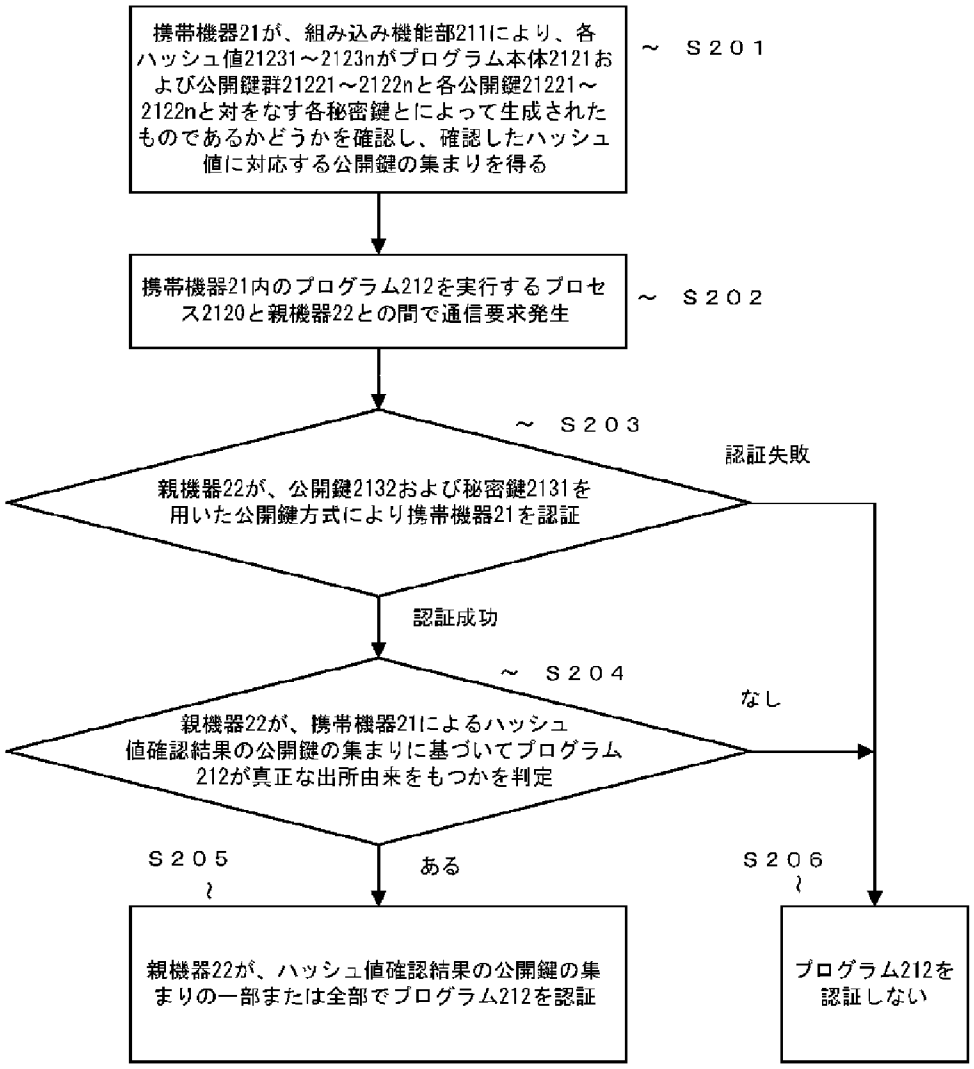
【図2】


携帯機器11が、組み込み機能部111により、ハッシュ値11231がプログラム本体1121と公開鍵11221と対をなす秘密鍵とによって生成されたものであることを確認
～ S101
携帯機器11内のプログラム112を実行するプロセス1120と親機器12との間で通信要求発生
～ S102
～ S103
親機器12が、公開鍵1132および秘密鍵1131を用いた公開鍵方式により携帯機器11を認証
認証失敗
認証成功
～ S104
親機器12が、携帯機器11によるハッシュ値確認結果に基づいてプログラム112が真正な出所由来をもつかを判定
いいえ
S105
はい
S106
親機器12が、公開鍵11221でプログラム112を認証したとする
プログラム112を認証しない

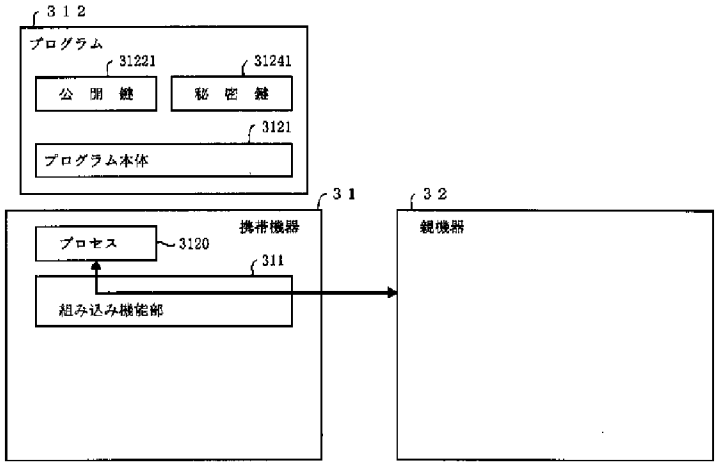
【図3】


212
プログラム
21221～2122n
21231～2123n
公開鍵
ハッシュ値
2121
プログラム本体
21
携帯機器
プロセス
2120
211
組み込み機能部
秘密鍵
2131
公開鍵
2132
22
親機器
公開鍵
2132

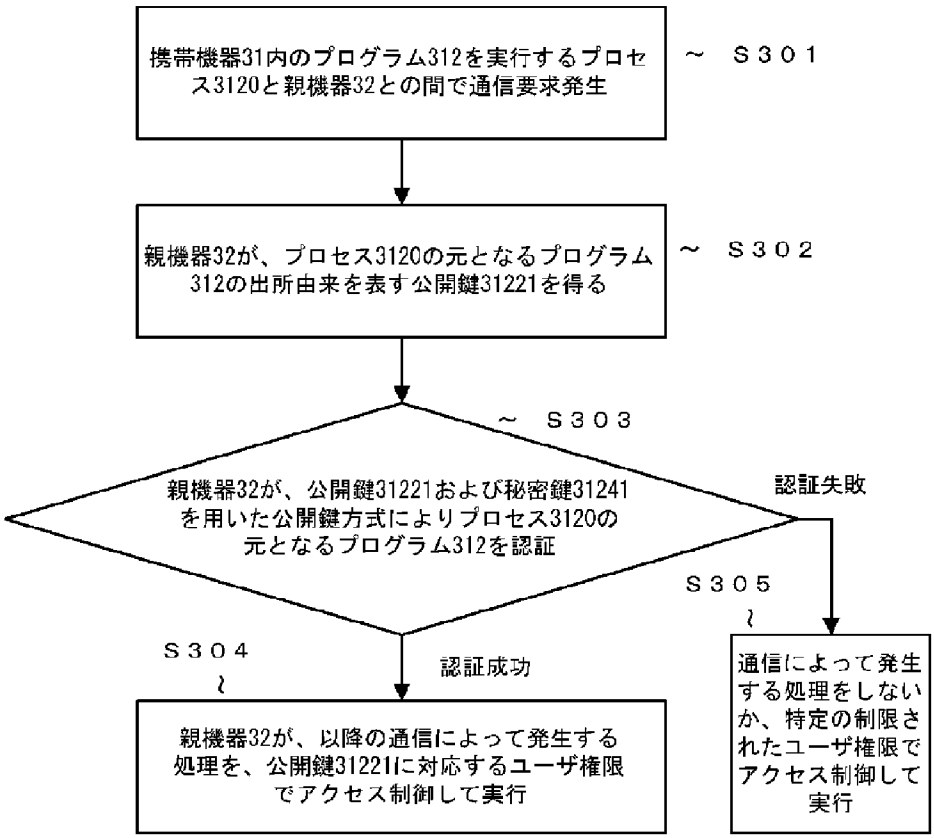
【図４】


携帯機器21が、組み込み機能部211により、各ハッシュ値21231～2123nがプログラム本体2121および公開鍵群21221～2122nと各公開鍵21221～2122nと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る
～ Ｓ２０１
携帯機器21内のプログラム212を実行するプロセス2120と親機器22との間で通信要求発生
～ Ｓ２０２
～ Ｓ２０３
親機器22が、公開鍵2132および秘密鍵2131を用いた公開鍵方式により携帯機器21を認証
認証失敗
認証成功
～ Ｓ２０４
親機器22が、携帯機器21によるハッシュ値確認結果の公開鍵の集まりに基づいてプログラム212が真正な出所由来をもつかを判定
なし
ある
Ｓ２０５
～
親機器22が、ハッシュ値確認結果の公開鍵の集まりの一部または全部でプログラム212を認証
Ｓ２０６
～
プログラム212を認証しない

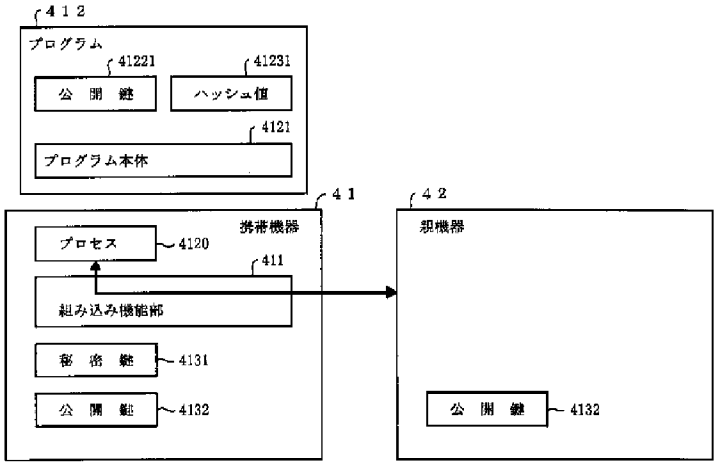
【図５】


３１２
プログラム
31221
公開鍵
31241
秘密鍵
3121
プログラム本体
３１
携帯機器
プロセス
3120
311
組み込み機能部
３２
親機器

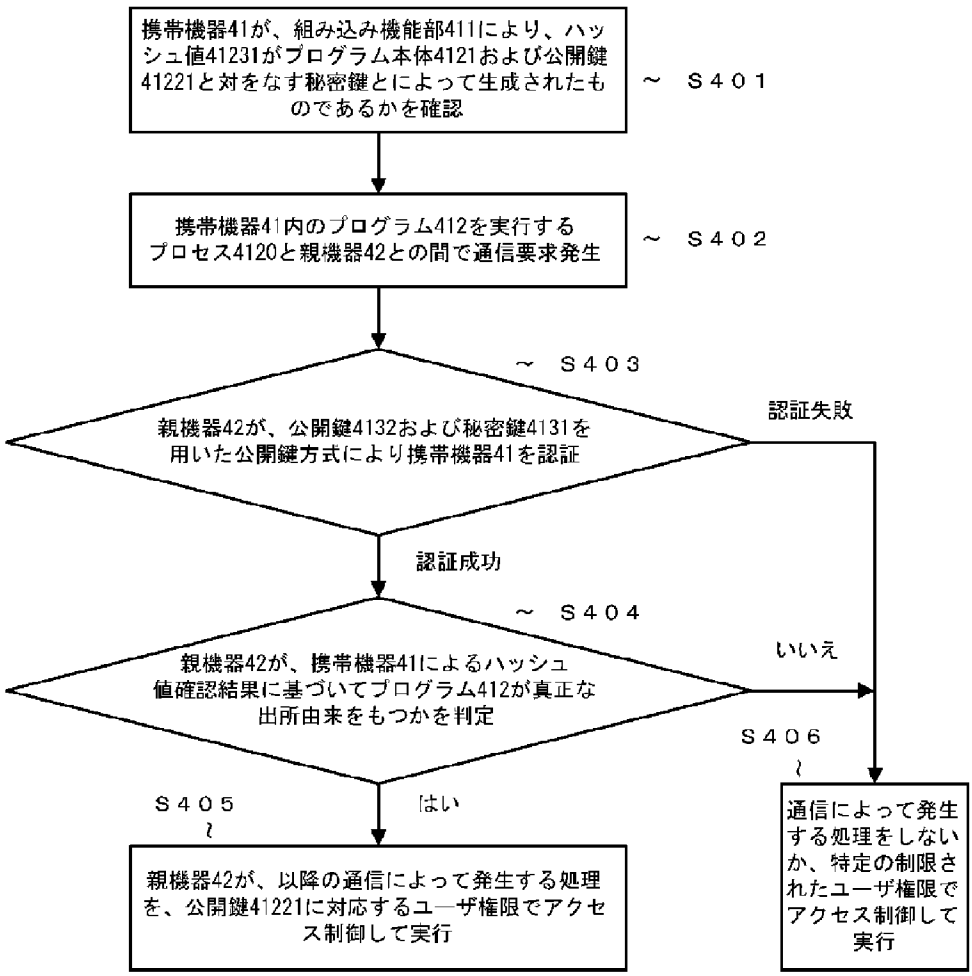
【図６】


携帯機器31内のプログラム312を実行するプロセス3120と親機器32との間で通信要求発生
～ Ｓ３０１
親機器32が、プロセス3120の元となるプログラム312の出所由来を表す公開鍵31221を得る
～ Ｓ３０２
～ Ｓ３０３
親機器32が、公開鍵31221および秘密鍵31241を用いた公開鍵方式によりプロセス3120の元となるプログラム312を認証
認証失敗
Ｓ３０５
通信によって発生する処理をしないか、特定の制限されたユーザ権限でアクセス制御して実行
Ｓ３０４
認証成功
親機器32が、以降の通信によって発生する処理を、公開鍵31221に対応するユーザ権限でアクセス制御して実行

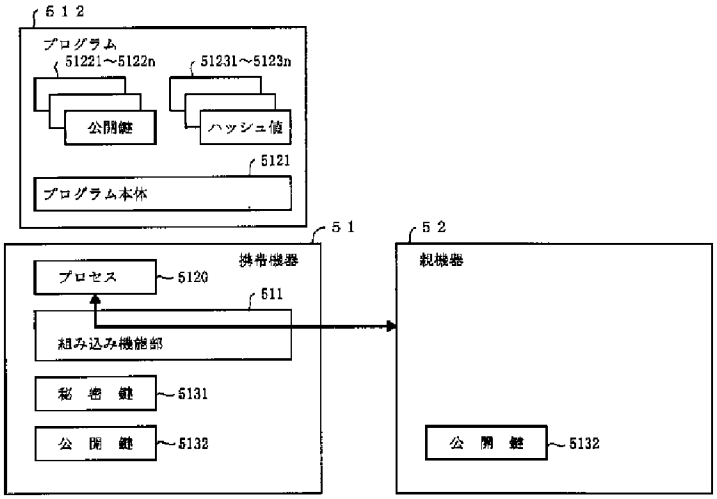
【図７】


４１２
プログラム
41221
41231
公開鍵
ハッシュ値
4121
プログラム本体
４１
携帯機器
プロセス
4120
411
組み込み機能部
秘密鍵
4131
公開鍵
4132
４２
親機器
公開鍵
4132

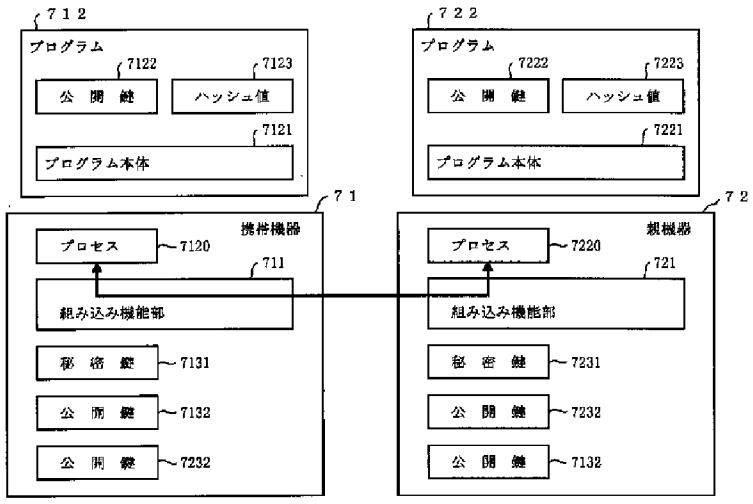
【図８】


携帯機器41が、組み込み機能部411により、ハッシュ値41231がプログラム本体4121および公開鍵41221と対をなす秘密鍵とによって生成されたものであるかを確認
～ Ｓ４０１
携帯機器41内のプログラム412を実行するプロセス4120と親機器42との間で通信要求発生
～ Ｓ４０２
～ Ｓ４０３
親機器42が、公開鍵4132および秘密鍵4131を用いた公開鍵方式により携帯機器41を認証
認証失敗
認証成功
～ Ｓ４０４
親機器42が、携帯機器41によるハッシュ値確認結果に基づいてプログラム412が真正な出所由来をもつかを判定
いいえ
Ｓ４０６
はい
Ｓ４０５
親機器42が、以降の通信によって発生する処理を、公開鍵41221に対応するユーザ権限でアクセス制御して実行
通信によって発生する処理をしないか、特定の制限されたユーザ権限でアクセス制御して実行

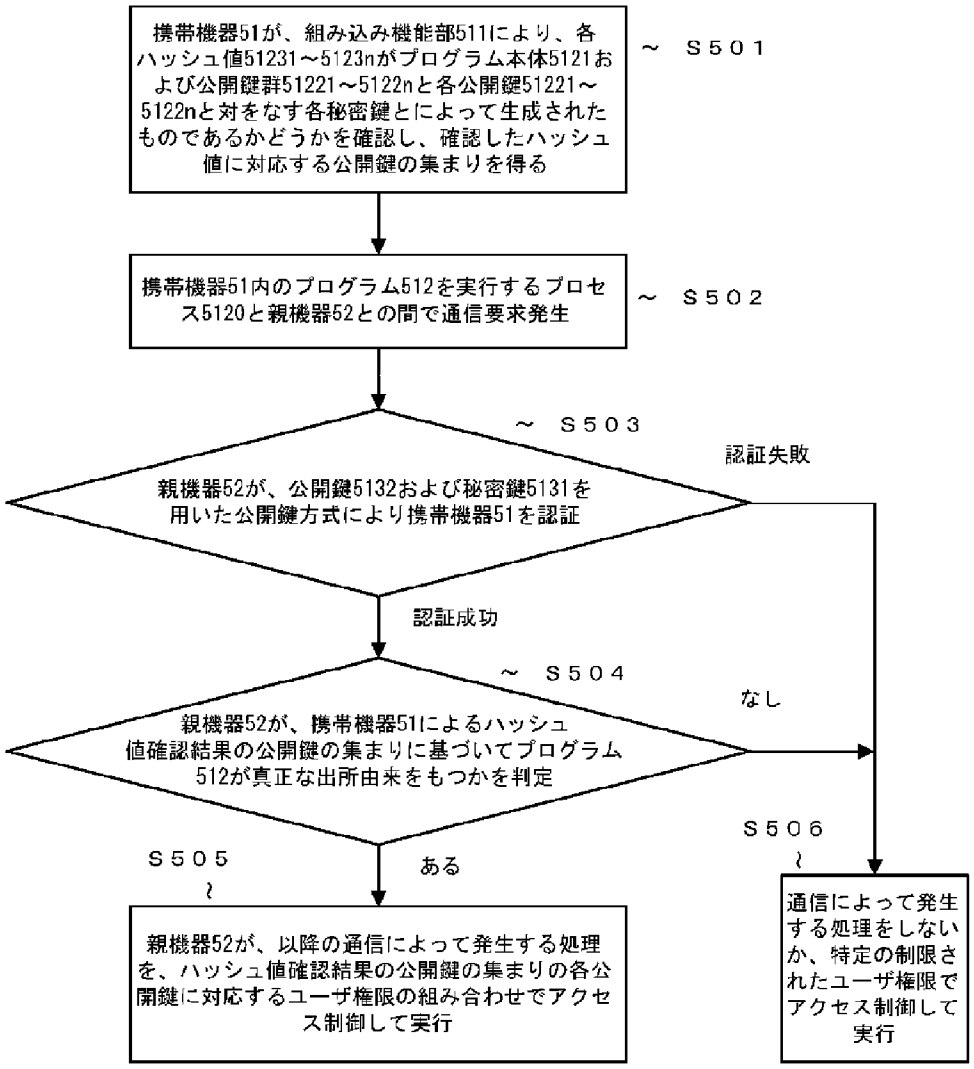
【図9】


512
プログラム
51221～5122n
51231～5123n
公開鍵
ハッシュ値
5121
プログラム本体
51
携帯機器
プロセス
5120
611
組み込み機能部
秘密鍵
5131
公開鍵
5132
52
親機器
公開鍵
5132

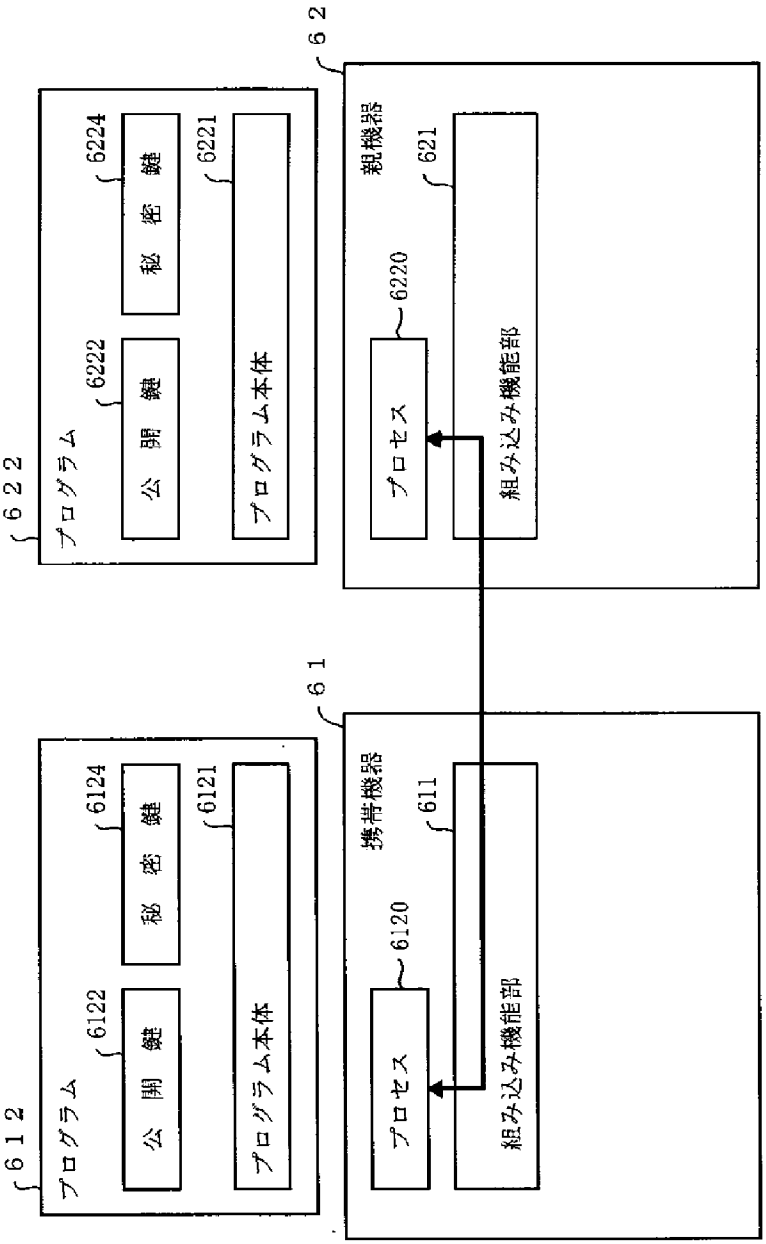
【図13】


712
プログラム
7122
7123
公開鍵
ハッシュ値
7121
プログラム本体
722
プログラム
7222
7223
公開鍵
ハッシュ値
7221
プログラム本体
71
携帯機器
プロセス
7120
711
組み込み機能部
秘密鍵
7131
公開鍵
7132
公開鍵
7232
72
親機器
プロセス
7220
721
組み込み機能部
秘密鍵
7231
公開鍵
7232
公開鍵
7132

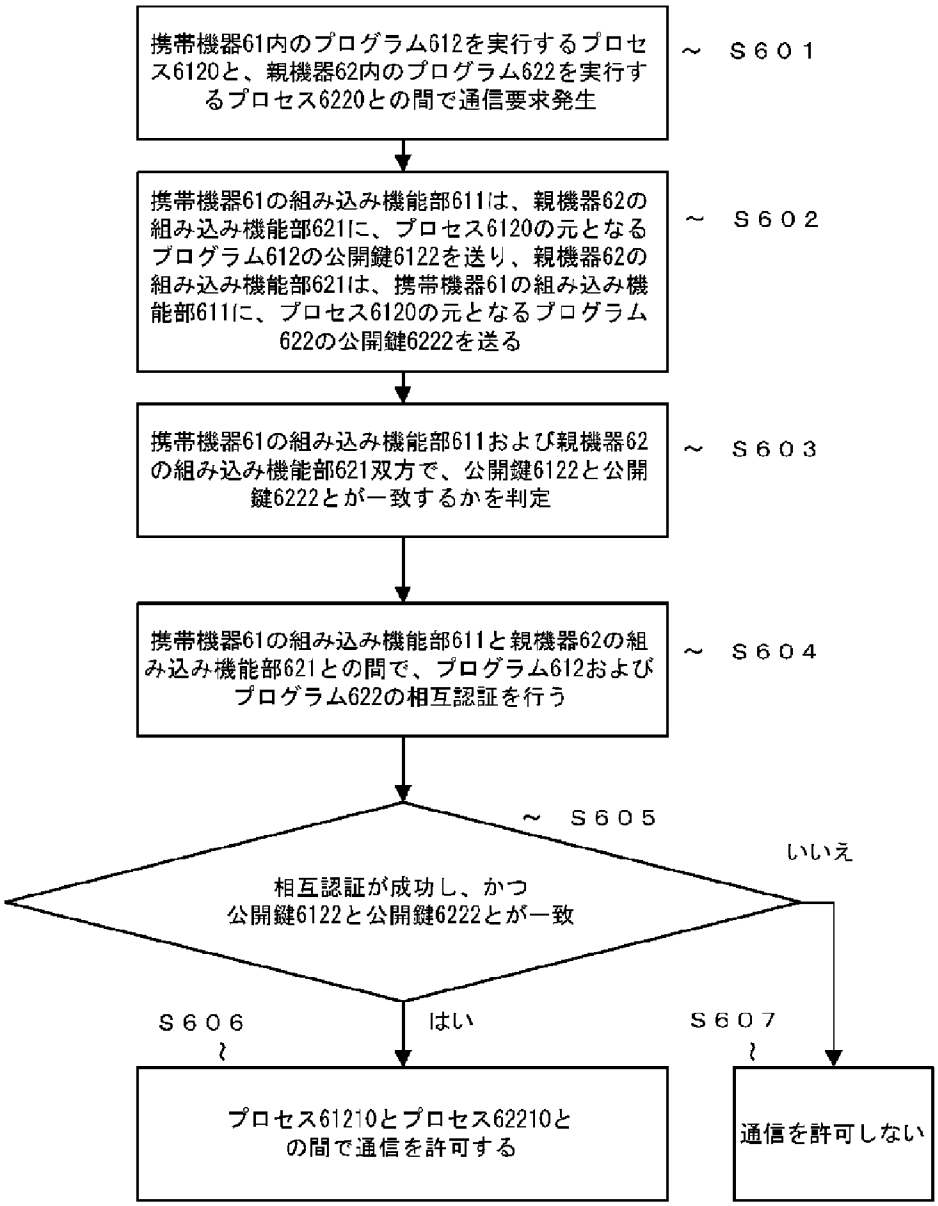
【図１０】


携帯機器51が、組み込み機能部511により、各ハッシュ値51231～5123nがプログラム本体5121および公開鍵群51221～5122nと各公開鍵51221～5122nと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る
～ Ｓ５０１
携帯機器51内のプログラム512を実行するプロセス5120と親機器52との間で通信要求発生
～ Ｓ５０２
～ Ｓ５０３
親機器52が、公開鍵5132および秘密鍵5131を用いた公開鍵方式により携帯機器51を認証
認証失敗
認証成功
～ Ｓ５０４
親機器52が、携帯機器51によるハッシュ値確認結果の公開鍵の集まりに基づいてプログラム512が真正な出所由来をもつかを判定
なし
ある
Ｓ５０５
～
親機器52が、以降の通信によって発生する処理を、ハッシュ値確認結果の公開鍵の集まりの各公開鍵に対応するユーザ権限の組み合わせでアクセス制御して実行
Ｓ５０６
～
通信によって発生する処理をしないか、特定の制限されたユーザ権限でアクセス制御して実行

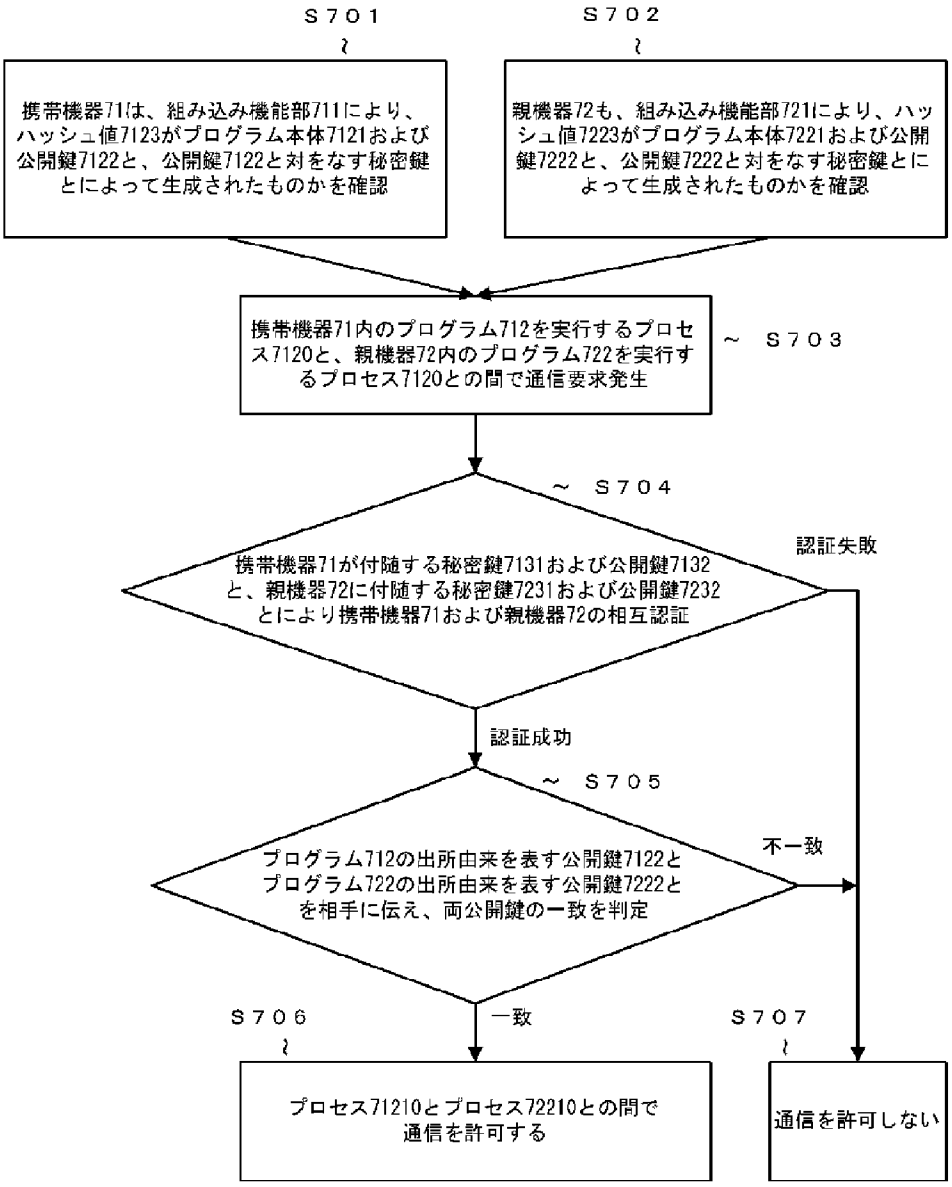
【図11】


62
親機器
621
6220
プロセス
組み込み機能部
622
プログラム
6222
公開鍵
6224
秘密鍵
6221
プログラム本体
61
携帯機器
611
6120
プロセス
組み込み機能部
612
プログラム
6122
公開鍵
6124
秘密鍵
6121
プログラム本体

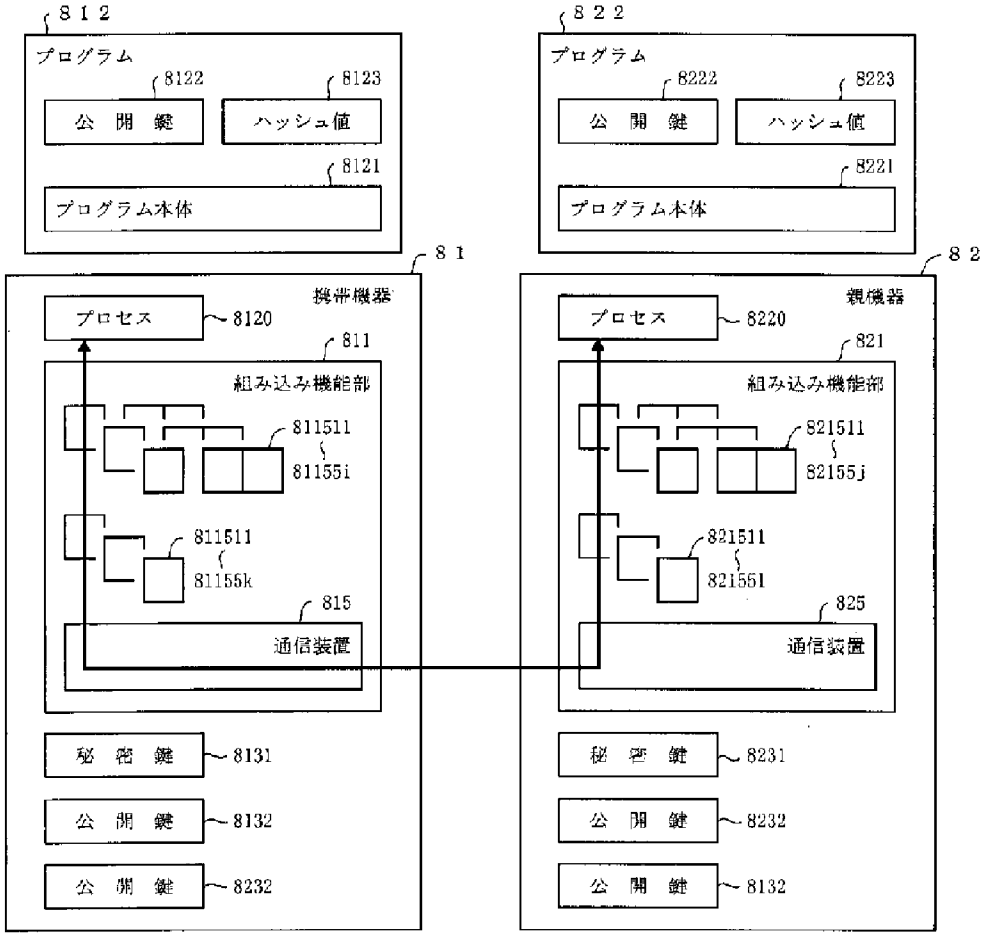
【図１２】


携帯機器61内のプログラム612を実行するプロセス6120と、親機器62内のプログラム622を実行するプロセス6220との間で通信要求発生
～ Ｓ６０１
携帯機器61の組み込み機能部611は、親機器62の組み込み機能部621に、プロセス6120の元となるプログラム612の公開鍵6122を送り、親機器62の組み込み機能部621は、携帯機器61の組み込み機能部611に、プロセス6120の元となるプログラム622の公開鍵6222を送る
～ Ｓ６０２
携帯機器61の組み込み機能部611および親機器62の組み込み機能部621双方で、公開鍵6122と公開鍵6222とが一致するかを判定
～ Ｓ６０３
携帯機器61の組み込み機能部611と親機器62の組み込み機能部621との間で、プログラム612およびプログラム622の相互認証を行う
～ Ｓ６０４
～ Ｓ６０５
相互認証が成功し、かつ
公開鍵6122と公開鍵6222とが一致
いいえ
はい
Ｓ６０６
～
Ｓ６０７
～
プロセス61210とプロセス62210との間で通信を許可する
通信を許可しない

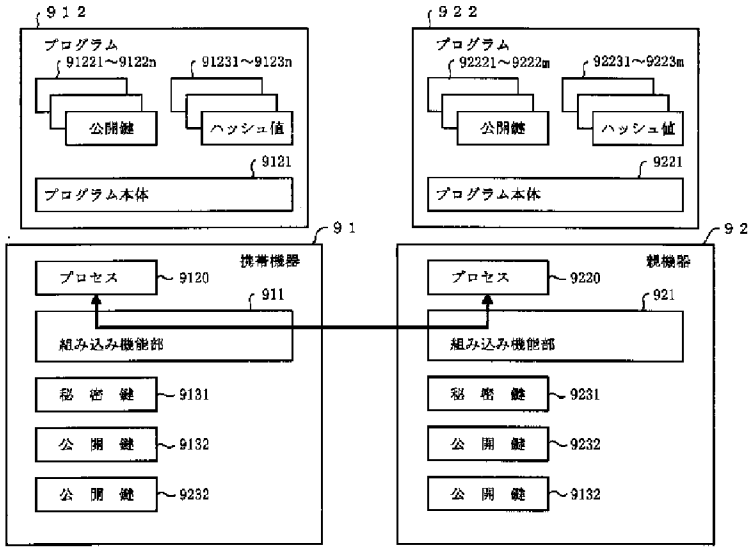
【図１４】


Ｓ７０１
携帯機器71は、組み込み機能部711により、ハッシュ値7123がプログラム本体7121および公開鍵7122と、公開鍵7122と対をなす秘密鍵とによって生成されたものかを確認
Ｓ７０２
親機器72も、組み込み機能部721により、ハッシュ値7223がプログラム本体7221および公開鍵7222と、公開鍵7222と対をなす秘密鍵とによって生成されたものかを確認
携帯機器71内のプログラム712を実行するプロセス7120と、親機器72内のプログラム722を実行するプロセス7120との間で通信要求発生
～ Ｓ７０３
～ Ｓ７０４
携帯機器71が付随する秘密鍵7131および公開鍵7132と、親機器72に付随する秘密鍵7231および公開鍵7232とにより携帯機器71および親機器72の相互認証
認証失敗
認証成功
～ Ｓ７０５
プログラム712の出所由来を表す公開鍵7122とプログラム722の出所由来を表す公開鍵7222とを相手に伝え、両公開鍵の一致を判定
不一致
一致
Ｓ７０６
プロセス71210とプロセス72210との間で通信を許可する
Ｓ７０７
通信を許可しない

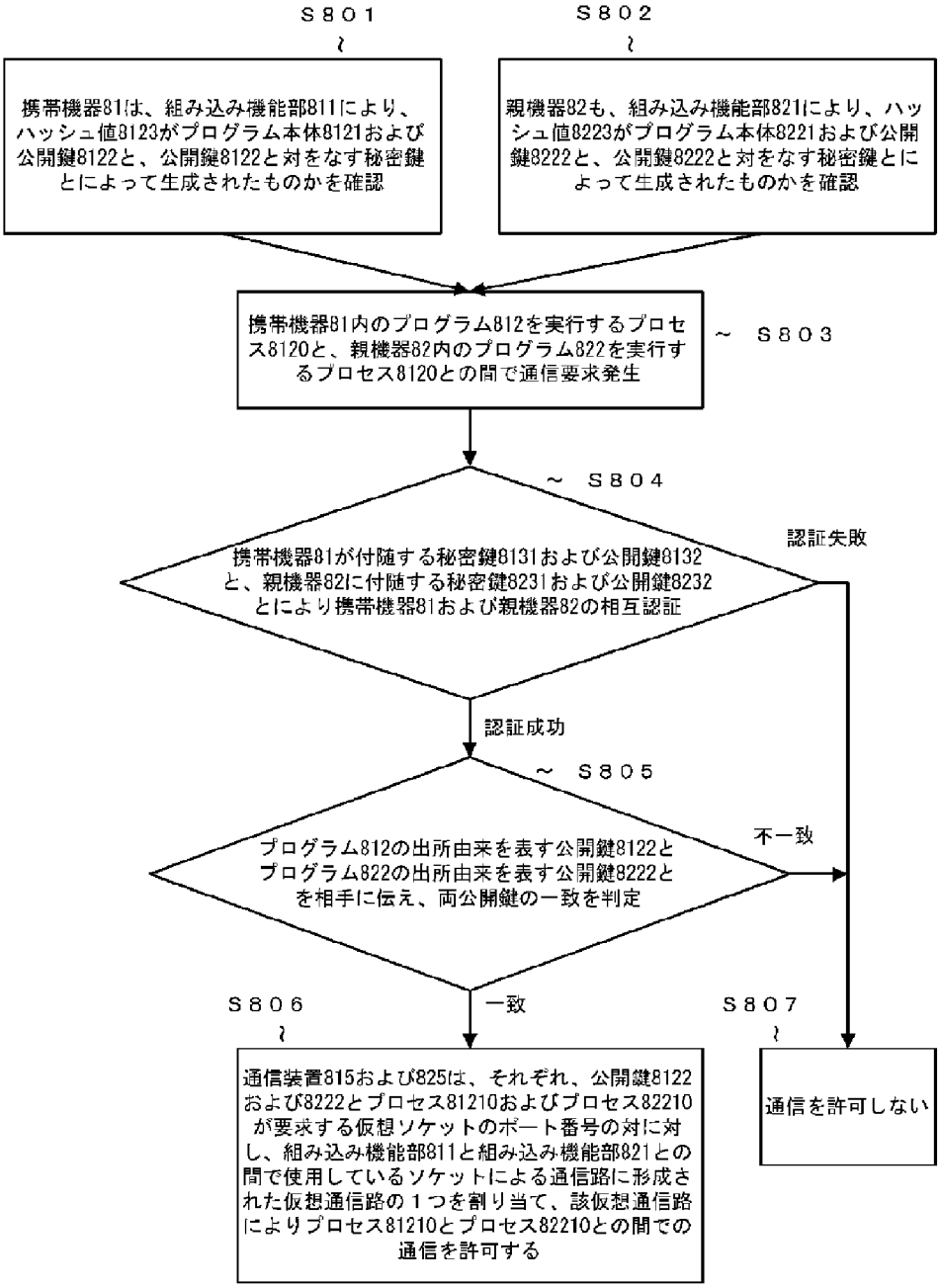
【図15】


812
プログラム
8122
公開鍵
8123
ハッシュ値
8121
プログラム本体
822
プログラム
8222
公開鍵
8223
ハッシュ値
8221
プログラム本体
81
携帯機器
プロセス
8120
811
組み込み機能部
811511
81155i
811511
81155k
815
通信装置
秘密鍵
8131
公開鍵
8132
公開鍵
8232
82
親機器
プロセス
8220
821
組み込み機能部
821511
82155j
821511
82155l
825
通信装置
秘密鍵
8231
公開鍵
8232
公開鍵
8132

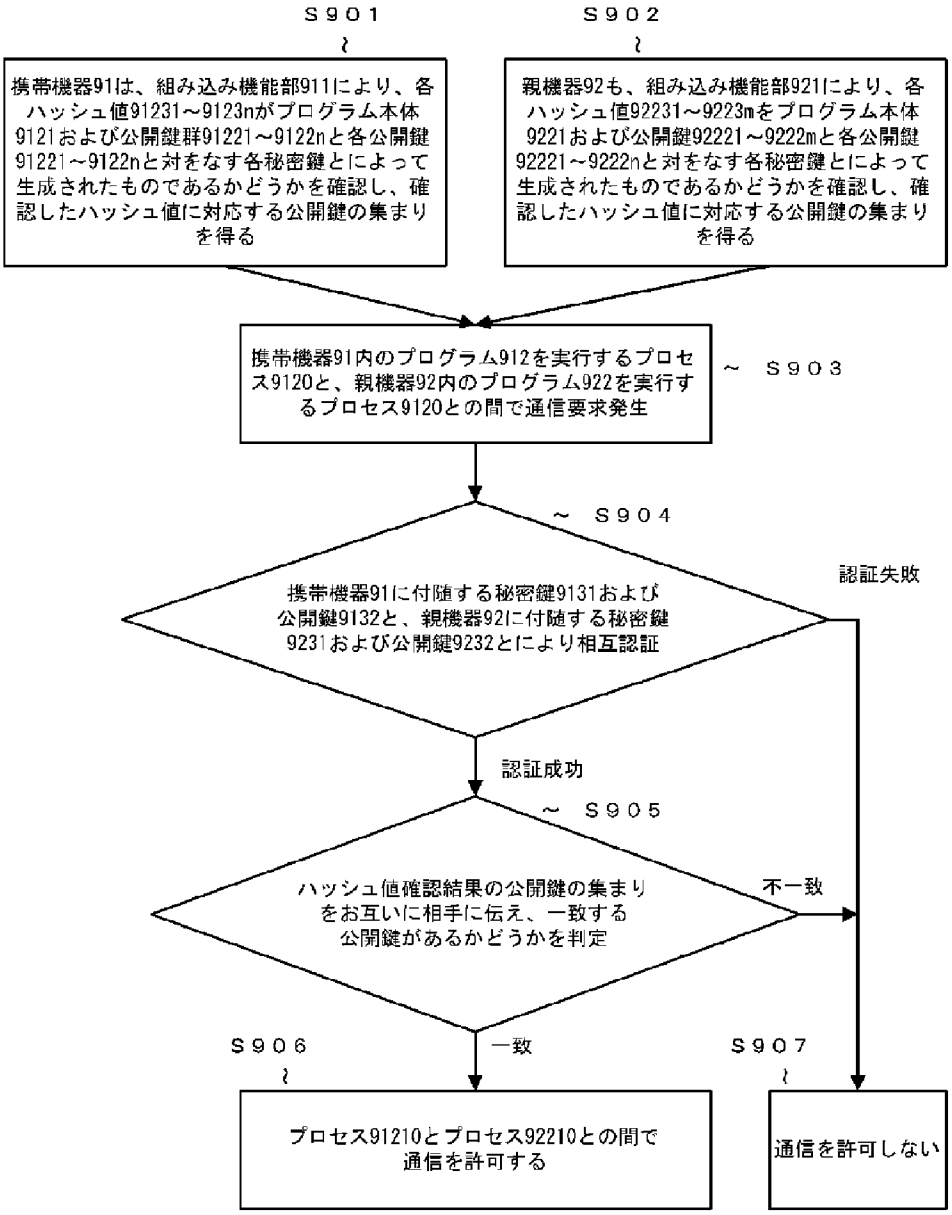
【図17】


912
プログラム
91221～9122n
公開鍵
91231～9123n
ハッシュ値
9121
プログラム本体
922
プログラム
92221～9222m
公開鍵
92231～9223m
ハッシュ値
9221
プログラム本体
91
携帯機器
プロセス
9120
911
組み込み機能部
秘密鍵
9131
公開鍵
9132
公開鍵
9232
92
親機器
プロセス
9220
921
組み込み機能部
秘密鍵
9231
公開鍵
9232
公開鍵
9132

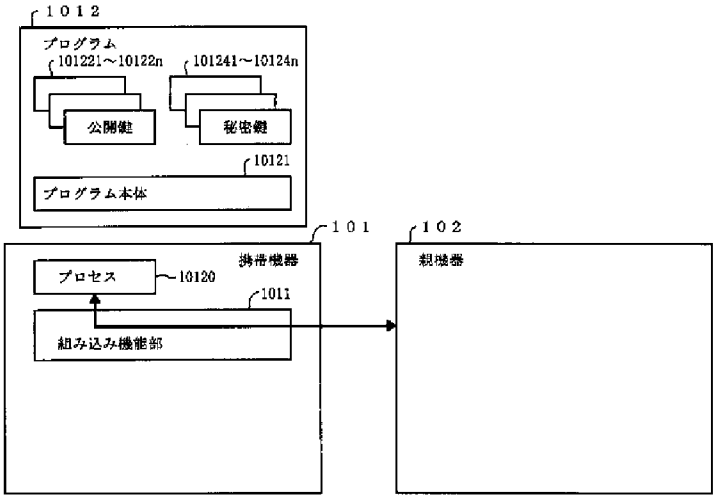
【図16】


S801
携帯機器81は、組み込み機能部811により、ハッシュ値8123がプログラム本体8121および公開鍵8122と、公開鍵8122と対をなす秘密鍵とによって生成されたものかを確認
S802
親機器82も、組み込み機能部821により、ハッシュ値8223がプログラム本体8221および公開鍵8222と、公開鍵8222と対をなす秘密鍵とによって生成されたものかを確認
携帯機器81内のプログラム812を実行するプロセス8120と、親機器82内のプログラム822を実行するプロセス8120との間で通信要求発生
～ S803
～ S804
携帯機器81が付随する秘密鍵8131および公開鍵8132と、親機器82に付随する秘密鍵8231および公開鍵8232とにより携帯機器81および親機器82の相互認証
認証失敗
認証成功
～ S805
プログラム812の出所由来を表す公開鍵8122とプログラム822の出所由来を表す公開鍵8222とを相手に伝え、両公開鍵の一致を判定
不一致
S806
一致
通信装置815および825は、それぞれ、公開鍵8122および8222とプロセス81210およびプロセス82210が要求する仮想ソケットのポート番号の対に対し、組み込み機能部811と組み込み機能部821との間で使用しているソケットによる通信路に形成された仮想通信路の１つを割り当て、該仮想通信路によりプロセス81210とプロセス82210との間での通信を許可する
S807
通信を許可しない

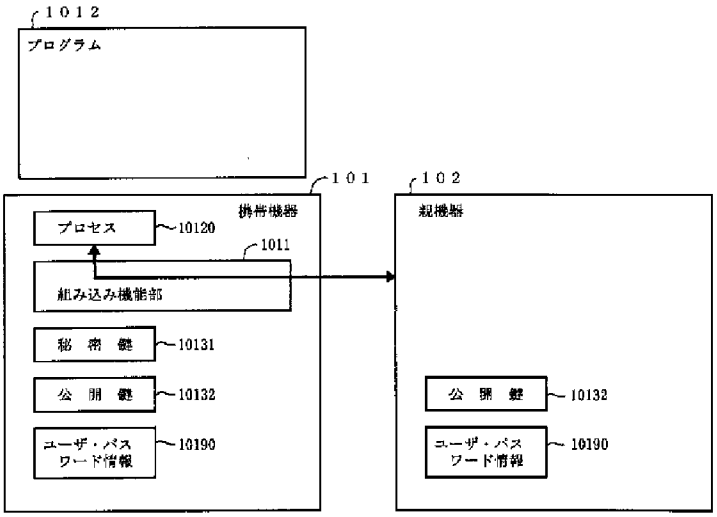
【図18】


S901
携帯機器91は、組み込み機能部911により、各ハッシュ値91231～9123nがプログラム本体9121および公開鍵群91221～9122nと各公開鍵91221～9122nと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る
S902
親機器92も、組み込み機能部921により、各ハッシュ値92231～9223mをプログラム本体9221および公開鍵92221～9222mと各公開鍵92221～9222nと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る
携帯機器91内のプログラム912を実行するプロセス9120と、親機器92内のプログラム922を実行するプロセス9120との間で通信要求発生
S903
S904
携帯機器91に付随する秘密鍵9131および公開鍵9132と、親機器92に付随する秘密鍵9231および公開鍵9232とにより相互認証
認証失敗
認証成功
S905
ハッシュ値確認結果の公開鍵の集まりをお互いに相手に伝え、一致する公開鍵があるかどうかを判定
不一致
S906
一致
S907
プロセス91210とプロセス92210との間で通信を許可する
通信を許可しない

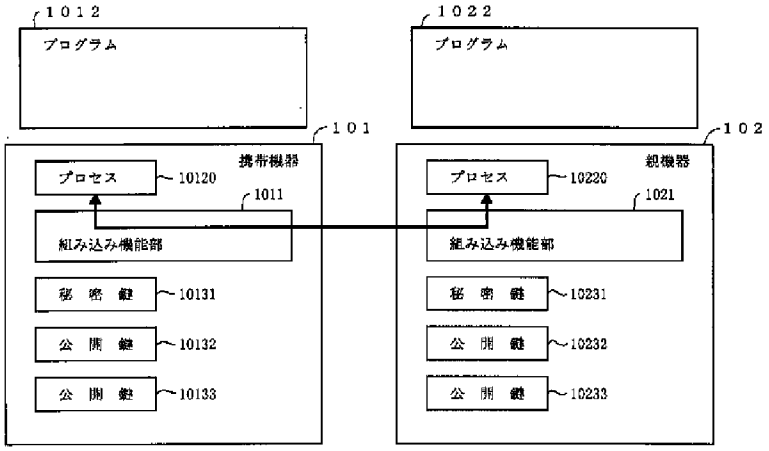
【図１９】


１０１２
プログラム
101221～10122n
101241～10124n
公開鍵
秘密鍵
10121
プログラム本体
１０１
携帯機器
プロセス
10120
1011
組み込み機能部
１０２
親機器

【図２０】


１０１２
プログラム
１０１
携帯機器
プロセス
10120
1011
組み込み機能部
秘密鍵
10131
公開鍵
10132
ユーザ・パスワード情報
10190
１０２
親機器
公開鍵
10132
ユーザ・パスワード情報
10190

【図21】


1012
プログラム
1022
プログラム
101
携帯機器
プロセス
10120
1011
組み込み機能部
秘密鍵
10131
公開鍵
10132
公開鍵
10133
102
親機器
プロセス
10220
1021
組み込み機能部
秘密鍵
10231
公開鍵
10232
公開鍵
10233

[Document Name] Description

[Title of the Invention] It is the channel offer method the secret-key-less program attestation method, the program ID communications processing control method, the program ID communication range control method, and the whole public key.

[Claim(s)]

[Claim 1] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus The public key and secret key with which said program execution and communication apparatus accompany this program execution and communication apparatus, Said program including the process generated and performed based on said program A program main part, The public key showing the source origin of this program and the signature performed to said program main part with this public key and the secret key which makes a pair are included. The process which said program execution and communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair, Before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program The process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus, When said signature is able to check being generated with the public key showing the source origin of said program main part and said

program, and the secret key which makes a pair The process which obtains the public key with which said communication and processing unit express the source origin of said program before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program, The secret-key-less program attestation method characterized by including the process for which this public key is attested with said communication and processing unit expressing the source origin of said program when the public key which succeeds in attestation of said program execution and communication apparatus, and expresses the source origin of said program is able to be obtained.

[Claim 2] In the process which said program execution and communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair It consists of a signature value enciphered with the public key with which said signature expresses the source origin of said program for the digest which carried out hashing of said program main part by the hash function, and the secret key which makes a pair. While said program execution and communication apparatus decode said signature value with the public key showing the source origin of said program and obtaining a digest, carry out hashing of said program main part by a hash function, and a digest is obtained. The secret-key-less program attestation method according to claim 1 characterized by judging whether both digests are in agreement.

[Claim 3] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus It is judged whether the public key which said communication and processing unit equip with the public key in which the partner who may communicate is shown and in which the partner who may this communicate is shown, and the public key which accompanies said program execution and communication apparatus are in agreement. The secret-key-less program attestation method according to claim 1 or 2 characterized by attesting said program execution and communication apparatus when in agreement.

[Claim 4] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The one-time password method by a public key is used, and [said communication and processing unit] Send a random character string to said program execution and communication apparatus, and [said program execution and communication apparatus] Encipher this character string with the secret key which accompanies this program execution and communication apparatus, return to said communication and processing unit, and [said communication and processing unit] The secret-key-less program attestation method according to claim 1 or 2 which will be characterized by attesting said program execution and communication apparatus if it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement.

[Claim 5] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus The public key and secret key with which said program execution and communication apparatus accompany this program execution and communication apparatus, Said program including the process generated and performed based on said program A program main part, The public key group showing the source origin of this program and the signature group performed with each public key and each secret key which makes a pair to the data created combining said program main part and said public key group are included. It is checked whether said program execution and communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair. Before communicating with the process which obtains a collection of the public keys corresponding to the signature by which being generated was checked with said communication and processing unit by processing of a process in which said program execution and communication apparatus were generated based on said program, [said communication and processing unit] The process which attests said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus, When one or more public keys corresponding to the signature by which said thing [being generated] was checked are obtained The process which obtains the public key with which said communication and processing unit express the source origin of said program before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program, When the public key which succeeds in attestation of said program execution and communication apparatus, and expresses the source origin of said program is able to be obtained The secret-key-less program attestation method characterized by including the process at which said communication and processing unit attest each public key of the signature check result by said program execution and communication apparatus with expressing the source origin of said program.

[Claim 6] It is checked whether said program execution and communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair. In the process which obtains a collection of the public keys corresponding to the checked signature Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created in the combination of said program main part and said public key group by the hash function, and each secret key which makes a pair, and [said program execution and communication apparatus] Carry out hashing of the data created in the combination of said program main part and said public key group while decoding each signature value with each public key showing the source origin of said program, respectively and obtaining the digest group by a hash function, and a digest is obtained. The secret-key-less program attestation method according to claim 5 characterized by judging whether this digest and said digest group are in agreement.

[Claim 7] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus It is judged whether the public key which said communication and processing unit equip with the public key in which the partner who may communicate is shown and in which the partner who may this communicate is shown, and the public key which accompanies said program execution and communication apparatus are in agreement. The secret-key-less program attestation method according to claim 5 or 6 characterized by attesting said program execution and communication apparatus when in agreement.

[Claim 8] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The one-time password method by a public key is used, and [said communication and processing unit] Send a random character string to said program execution and communication apparatus, and [said program execution and communication apparatus] Encipher this character string with the secret key which accompanies this program execution and communication apparatus, return to said communication and processing unit, and [said communication and processing unit] The secret-key-less program attestation method according to claim 5 or 6 which will be characterized by attesting said program execution and communication apparatus if it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement.

[Claim 9] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus Said program contains a program main part and ID group showing the source origin of this program. Said program execution and communication apparatus include the process generated and performed based on said program. Before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program When one or more ID(s) which express said source origin as the process which obtains a part or all of ID group to which said communication and processing unit express the source origin of the program which becomes the origin of said process are obtained In the processing which said communication and processing unit generated by the process which communicates with said program execution and communication apparatus by processing of the process generated based on said program, and communication The program ID communications processing control method characterized by including the process which performs access control carried out based on ID group to which said communication and processing unit express said source origin obtained from said program execution and management equipment.

[Claim 10] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the

communication and the processing unit which communicate with this program execution and communication apparatus Said program contains a program main part, the public key showing the source origin of this program, and this public key and the secret key which makes a pair. Said program execution and communication apparatus include the process generated and performed based on said program. Before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program The process which obtains the public key with which said communication and processing unit express the source origin of said program which consists of said program execution and communication apparatus the origin of the process which makes this program execution and communication apparatus communicate, When said program is attested with the process with which said communication and processing unit attest said program with the public key method using the public key and secret key showing the source origin of said program The program ID communications processing control method characterized by said communication and processing unit including the process which communicates with said program execution and communication apparatus by access control carried out based on said public key.

[Claim 11] In the process with which said communication and processing unit attest said program about the obtained public key with the public key method using the public key and secret key showing the source origin of said program The one-time password method by a public key is used, and [said program execution and communication apparatus] Send said public key to said communication and processing unit, and said communication and processing unit send a random character string to said program execution and communication apparatus. Said program execution and communication apparatus return the character string which enciphered this character string with said secret key to said communication and processing unit. The program ID communications processing control method according to claim 10 which will be characterized by attesting said program if said communication and processing unit decode the enciphered character string with said sent public key and the decoded character string and the character string sent previously are in agreement.

[Claim 12] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus The public key and secret key with which said program execution and communication apparatus accompany this program execution and communication apparatus, Said program including the process generated and performed based on said program A program main part, The public key showing the source origin of this program and the signature performed to said program main part with this public key and the secret key which makes a pair are included. The process which said program execution and communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair, Before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program The process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which

accompany said program execution and communication apparatus, When said signature is able to check being generated with the public key showing the source origin of said program main part and said program, and the secret key which makes a pair The process which obtains the public key with which said communication and processing unit express the source origin of said program before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program, When the public key which succeeds in attestation of said program execution and communication apparatus, and expresses the source origin of said program is able to be obtained The program ID communications processing control method characterized by including the process which communicates with said program execution and communication apparatus by access control which said communication and processing unit obtained the public key showing the source origin of said program from said program execution and communication apparatus, and carried out based on this public key.

[Claim 13] In the process which said program execution and communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair It consists of a signature value enciphered with the public key with which said signature expresses the source origin of said program for the digest which carried out hashing of said program main part by the hash function, and the secret key which makes a pair. While said program execution and communication apparatus decode said signature value with the public key showing the source origin of said program and obtaining a digest, carry out hashing of said program main part by a hash function, and a digest is obtained. The program ID communications processing control method according to claim 12 characterized by judging whether both digests are in agreement.

[Claim 14] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The program ID communications processing control method according to claim 12 or 13 characterized by judging whether the public key with which said communication and processing unit are equipped with the public key in which the partner who may communicate is shown, and accompanies said program execution and communication apparatus, and the public key in which said partner who may communicate is shown are in agreement.

[Claim 15] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The one-time password method by a public key is used, and [said communication and processing unit] Send a random character string to said program execution and communication apparatus, and [said program execution and communication apparatus] Encipher this character string with the secret key which accompanies this program execution and communication apparatus, return to said communication and processing unit, and [said communication and processing unit] The program ID communications processing control method

according to claim 12 or 13 which will be characterized by attesting said program execution and communication apparatus if it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement.

[Claim 16] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus The public key and secret key with which said program execution and communication apparatus accompany this program execution and communication apparatus, Said program including the process generated and performed based on said program A program main part, The public key group showing the source origin of this program and the signature group performed with each public key and each secret key which makes a pair to the data created combining said program main part and said public key group are included. It is checked whether said program execution and communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair. Before communicating with the process which obtains a collection of the public keys corresponding to the signature by which being generated was checked with said communication and processing unit by processing of a process in which said program execution and communication apparatus were generated based on said program, [said communication and processing unit] The process which attests said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus, When one or more public keys corresponding to the signature by which said thing [being generated] was checked are obtained The process which obtains the public key with which said communication and processing unit express the source origin of said program before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program, When the public key which succeeds in attestation of said program execution and communication apparatus, and expresses the source origin of said program is able to be obtained The program ID communications processing control method characterized by including the process which communicates with said program execution and communication apparatus by access control which said communication and processing unit carried out based on a part or all of a collection of public keys of a signature check result by said program execution and communication apparatus.

[Claim 17] In the process which checks whether said program execution and communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created combining said program main part and said public key group by the hash function, and each secret key which makes a pair, and [said program execution and communication apparatus] Each digest which decoded each signature value with each public key, respectively, The program ID communications

processing control method according to claim 16 characterized by judging whether the digest obtained by carrying out hashing of the data created combining said program main part and said public key group by a hash function is in agreement.

[Claim 18] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The program ID communications processing control method according to claim 16 or 17 characterized by judging whether the public key with which said communication and processing unit are equipped with the public key in which the partner who may communicate is shown, and accompanies said program execution and communication apparatus, and the public key in which said partner who may communicate is shown are in agreement.

[Claim 19] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The one-time password method by a public key is used, and [said communication and processing unit] Send a random character string to said program execution and communication apparatus, and [said program execution and communication apparatus] Encipher this character string with the secret key which accompanies this program execution and communication apparatus, return to said communication and processing unit, and [said communication and processing unit] The program ID communications processing control method according to claim 16 or 17 which will be characterized by attesting said program execution and communication apparatus if it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement.

[Claim 20] In the information system constituted by the program, and two or more program execution and communication apparatus which generate a process, respectively and perform it based on these programs Said program contains a program main part and ID group showing the source origin of this program. [a certain process which the program execution and the communication apparatus which exists based on a certain program generated] Before communicating with a certain another process to which another a certain program execution and communication apparatus generated this program or a certain another program to origin When ID group which expresses said source origin as the process which obtains a part or all of ID group to which both program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in partner program execution and a communication apparatus is obtained ID group showing the source origin of said program which becomes ID group to which both program execution and a communication apparatus express the obtained source origin, and the origin of the process in self-program execution and a communication apparatus is compared. The program ID communication range control method characterized by including the process which will open a channel if one or more ID(s) showing the source origin of said program in agreement exist.

[Claim 21] In the information system constituted by the program, and two or more program execution and communication apparatus which generate and perform each process based on each program Said program contains a program main part, the public key showing the source origin of this program, and this public key and the secret key which makes a pair. [a certain process which the program execution and the communication apparatus which exists based on a certain program generated] Before communicating with a certain another process to which another a certain program execution and communication apparatus generated this program or a certain another program to origin The process which obtains the public key with which both program execution and a communication apparatus express the source origin of said program which consists of partner program execution and a communication apparatus the origin of the process in partner program execution and a communication apparatus, respectively, [the process which judges whether the public key with which both program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication apparatus, and self-program execution and a communication apparatus is in agreement, and both program execution and a communication apparatus] The process which performs mutual recognition of the program which becomes the origin of the process in partner program execution and a communication apparatus using the public key and secret key showing the source origin of said program which becomes the origin of the process in partner program execution and a communication apparatus, The public key showing the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication apparatus, and self-program execution and a communication apparatus is in agreement. And the program ID communication range control method characterized by both program execution and a communication apparatus including the process which opens a channel when mutual recognition of the program which becomes the origin of the process in partner program execution and a communication apparatus is carried out.

[Claim 22] In the process which performs mutual recognition of the program which becomes the origin of the process in partner program execution and a communication apparatus using the public key and secret key with which both program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in partner program execution and a communication apparatus The one-time password method by a public key is used, and [both program execution and a communication apparatus] The public key which accompanies self-program execution and a communication apparatus is sent to partner program execution and a communication apparatus. A random character string is sent to partner program execution and a communication apparatus, respectively. The character string enciphered with the public key with which partner program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in partner program execution and a communication apparatus about this character string, and the secret key which makes a pair is returned to self-program execution and a communication apparatus. If self-program execution and a communication apparatus decode the enciphered character string with a corresponding public key and the decoded character string and the character string sent previously are in agreement The program ID communication range control method according to claim 21 characterized by attesting the program which becomes the origin of the process in partner program execution and a

communication apparatus communication apparatus.

[Claim 23] In the information system constituted by the program, and two or more program execution and communication apparatus which generate and perform each process based on each program The public key and secret key with which said program execution and communication apparatus accompany self-program execution and a communication apparatus, Said program including the public key which accompanies partner program execution and a communication apparatus, and the process generated and performed based on said program A program main part, The public key showing the source origin of this program and the signature performed to said program main part with this public key and the secret key which makes a pair are included. [a certain process which the program execution and the communication apparatus which exists based on a certain program generated] Before communicating with a certain another process to which another a certain program execution and communication apparatus generated this program or a certain another program to origin Before said signature performs said communication with the process which checks whether it is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair, both program execution and a communication apparatus [both program execution and a communication apparatus] The process which attests partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus, When both program execution and a communication apparatus are able to check that said signature is generated with the public key showing the source origin of said program main part and said program, and the secret key which makes a pair The process which transmits said public key to partner program execution and a communication apparatus before performing said communication, The process which judges whether the public key with which both program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication apparatus, and self-program execution and a communication apparatus is in agreement, Mutual recognition of the program which becomes the origin of the process in partner program execution and a communication apparatus is carried out. When [and] the public key showing the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication apparatus, and self-program execution and a communication apparatus is in agreement The program ID communication range control method characterized by both program execution and a communication apparatus including the process which opens a channel.

[Claim 24] In the process which both program execution and a communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair It consists of a signature value enciphered with the public key with which said signature expresses the source origin of said program for the digest which carried out hashing of said program main part by the hash function, and the secret key which makes a pair. While both program execution and a communication apparatus decode said signature value with the public key showing the source origin of said program and obtaining a digest, carry out hashing of said program main part by a hash function, and a digest is obtained. The program ID communication range control method according to claim 23 or 24 characterized by judging whether both digests are in

agreement.

[Claim 25] In the process with which both program execution and a communication apparatus attest partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus Both program execution and a communication apparatus are equipped with the public key in which the partner who may communicate is shown. The program ID communication range control method according to claim 23 or 24 characterized by judging whether the public key in which the this partner who may communicate is shown, and one or more public keys of the public key group which accompanies partner program execution and a communication apparatus are in agreement.

[Claim 26] In the process with which both program execution and a communication apparatus attest partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus The one-time password method by a public key is used, and [self-program execution and a communication apparatus] The public key which accompanies partner program execution and a communication apparatus is obtained from partner program execution and a communication apparatus. Send a random character string to partner program execution and a communication apparatus, and [partner program execution and a communication apparatus] Encipher this character string with the secret key which accompanies partner program execution and a communication apparatus, return to self-program execution and a communication apparatus, and [self-program execution and a communication apparatus] The program ID communication range control method according to claim 23 or 24 which will be characterized by attesting partner program execution and a communication apparatus if the enciphered character string is decoded with said public key obtained from partner program execution and a communication apparatus and the decoded character string and the character string sent previously are in agreement.

[Claim 27] When there is a public key where both program execution and a communication apparatus succeed in attestation of partner program execution and a communication apparatus, and corresponds with a collection of the public keys of the signature check result by both program execution and a communication apparatus The communication apparatus with which both program execution and a communication apparatus form two or more virtual channels in per channel virtually in the process which opens the channel between processes, The resource group for virtual channels showing the source origin of said program which exists for every public key, When the public key showing the source origin of said program is obtained including the resource group for channels When the process generated based on said program communicates, [the communication apparatus of both program execution and a communication apparatus] The program ID communication range control method according to claim 26 characterized by assigning channel resources to one of the virtual channel resource groups corresponding to the public key showing the obtained source origin, and offering a channel using virtual channel resources.

[Claim 28] In the information system constituted by the program, and two or more program execution and communication apparatus which generate and perform each process based on each program The public key and secret key with which said program execution and communication apparatus accompany self-program execution and a communication apparatus, Each program including the public key which accompanies partner program execution and a communication apparatus, and the process generated and performed based on each program A program main part, The public key group showing the source origin of this program and the signature group performed with each public key and each secret key which makes a pair to the data created combining said program main part and said public key group are included. [the process which checks whether both program execution and a communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair, and both program execution and a communication apparatus] [the process which attests partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus, and both program execution and a communication apparatus] A collection of the public keys of the signature check result by self-program execution and a communication apparatus is told to partner program execution and a communication apparatus. The process which judges whether there is any public key which is in agreement with a collection of the public keys of the signature check result by self-program execution and a communication apparatus and a collection of the public keys of the signature check result by partner program execution and a communication apparatus, One or more public keys which succeed in attestation of partner program execution and a communication apparatus, and are in agreement with a collection of the public keys of the signature check result by both program execution and a communication apparatus at a certain time The program ID communication range control method characterized by both program execution and a communication apparatus including the process which opens the channel between processes.

[Claim 29] In the process which judges whether both program execution and a communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created combining said program main part and said public key group by the hash function, and each secret key which makes a pair, and [partner program execution and a communication apparatus] Carry out hashing of the data created by said program main part and said public key group while decoding each signature value with each public key showing the source origin of said program, respectively and obtaining the digest group by a hash function, and a digest is obtained. The program ID communication range control method according to claim 28 characterized by judging whether this digest and said digest group are in agreement.

[Claim 30] In the process with which both program execution and a communication apparatus attest partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus Both

program execution and a communication apparatus are equipped with the public key in which the partner who may communicate is shown. The program ID communication range control method according to claim 28 or 29 characterized by judging whether the public key in which the this partner who may communicate is shown, and one or more public keys of the public key group which accompanies partner program execution and a communication apparatus are in agreement.

[Claim 31] In the process with which both program execution and a communication apparatus attest partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus The one-time password method by a public key is used, and [self-program execution and a communication apparatus] The public key which accompanies partner program execution and a communication apparatus is obtained from partner program execution and a communication apparatus. Send a random character string to partner program execution and a communication apparatus, and [partner program execution and a communication apparatus] Encipher this character string with the secret key which accompanies partner program execution and a communication apparatus, return to self-program execution and a communication apparatus, and [self-program execution and a communication apparatus] The program ID communication range control method according to claim 28 or 29 which will be characterized by attesting partner program execution and a communication apparatus if the enciphered character string is decoded with said public key obtained from partner program execution and a communication apparatus and the decoded character string and the character string sent previously are in agreement.

[Claim 32] When there is a public key where both program execution and a communication apparatus succeed in attestation of partner program execution and a communication apparatus, and corresponds with a collection of the public keys of the signature check result by both program execution and a communication apparatus The communication apparatus with which both program execution and a communication apparatus form two or more virtual channels in per channel virtually in the process which opens the channel between processes, The resource group for virtual channels showing the source origin of said program which exists for every public key, When one or more public keys showing the source origin of said program are obtained including the resource group for channels When the process generated based on said program communicates, [the communication apparatus of both program execution and a communication apparatus] The program ID communication range control method according to claim 31 characterized by assigning channel resources to one of the virtual channel resource groups corresponding to the public key showing the obtained source origin, and offering a channel using virtual channel resources.

[Claim 33] The resource group for virtual channels is the socket defined virtually, and it corresponds to each port of the socket which each of these virtual channel resource groups defined as this virtual target. The program ID communication range control method according to claim 27 or 32 which the resource group for channels is the usual socket, and is characterized by each of each channel resource groups corresponding to this socket each usual port.

[Claim 34] In the information system constituted by the program, and the program execution and the communication apparatus which generate a process based on this program, and perform and communicate Said program including the process in which said program execution and communication apparatus are generated and performed based on said program A program main part, The public key showing the source origin of this program, and the communication apparatus which forms two or more virtual channels in per channel virtually, The resources for virtual channels which exist for every public key showing the source origin of said program, When said program execution and communication apparatus communicate by processing of the process generated based on said program including one or more resources for channels It is the channel offer method the whole public key which makes a pair the resources for virtual channels required as the public key showing the source origin, and is characterized by including ****** which is made to correspond with a virtual channel and offers a channel using a virtual channel.

[Claim 35] The resource group for virtual channels is the socket defined virtually, and it corresponds to each port of the socket which each of these virtual channel resource groups defined as this virtual target. It is the channel offer method the whole public key according to claim 34 which the resource group for channels is the usual socket, and is characterized by each of each channel resource groups corresponding to this socket each usual port.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the program attestation method, the access control method of the processing generated by communication between programs in distributed environment, and the communication range control method of the program in distributed environment.

[0002]

[Description of the Prior Art] The program 1012 constituted by the pair of the public key groups 101221-10122n and the secret keys 101241-10124n with which an example of the conventional information system expresses the program main part 10121 and the source origin of a program 1012 as shown, for example in drawing 19, Are constituted by the process 10120 generated and performed by the portable device 101 which are program execution and a communication apparatus based on a program 1012. The principal part was constituted by the portable device 101 which generates and performs a process 10120 for a program 1012 based on a program 1012, and the main phone machine 102 which are the communication and the processing unit which communicates with the portable device 101.

[0003] As shown, for example in drawing 19, an example of the conventional information system A program 1012, The principal part consisted of a portable device 101 which are the program execution and the communication apparatus which generates and performs a process 10120 based on a program 1012, and a main phone machine 102 which are the communication and the processing unit which communicates with the portable device 101.

[0004] The program 112 was constituted including the program main part 10121, the public key groups 101221-10122n showing the source origin of a program 1012, and the public key groups 101221-10122n and the secret keys 101241-10124n which make a pair.

[0005] The portable device 101 consisted of an inclusion functional part 1011, a process 10120 which executes a program 1012, a public key 10132 which accompanies the portable device 101, a public key 10132 and the secret key 10131 which makes a pair, and user password information 10190.

[0006] The main phone machine 102 was constituted including the public key 10132 which accompanies the portable device 101 which is ID showing the partner who may communicate, and the user password information 10190 that the user who may communicate is expressed.

[0007] Before the portable device 101 communicates with the main phone machine 102 in such a conventional information system by processing of the process 10120 generated based on the program 1012 The process which obtains the public keys 101221-10122n with which the main phone machine 102 expresses the source origin of the program 1012 which consists of a portable device 101 the origin of the process 10120 which makes the portable device 101 communicate, [the main phone machine 102 / public keys / 101221-10122n / which were obtained / each] [attesting by making the public key groups 101221-10122n and the secret keys 101241-10124n showing the source origin of the program 1012 which becomes the origin of the process 10120 which makes the portable device 101 communicate used] It was attesting, when the program 1012 which becomes the origin of a process 10120 had all the public keys that succeeded in attestation.

[0008] Moreover, as other examples of an information system are conventionally shown, for example in drawing 20 The principal part consisted of a program 1012, a portable device 101 which are the program execution and the communication apparatus which generates and performs a process 10120 based on a program 1012, and a main phone machine 102 which are the communication and the processing unit which communicates with the portable device 101.

[0009] The portable device 101 consisted of an inclusion functional part 1011, a process 10120 which executes a program 1012, the public key 10132 and secret key 10131 which accompany the portable device 101, and user password information 10190.

[0010] The main phone machine 102 has the public key 10132 which accompanies the portable device 101 as a public key in which the partner who may communicate is shown, and the user password information 10190.

[0011] In such a conventional information system, with the portable device 101, it attests about the user password information 10190, and the process 10120 which executes a program 1012 holds the user password information 10190. When a process 10120 tends to communicate with the main phone machine 102 and a communication demand occurs, [the main phone machine 102] If a public key 10132 is received from the portable device 101 and it is in agreement with a public key 10132 When it attests about a public key 10132 to the portable device 101 and succeeds in attestation [the access control about the processing which allows communication with the process 10120 and the main phone machine 102 which execute the program 1012 in the portable device 101, and is generated by the communication] The user password information 10190 which is not based on a communication partner, but performs the same access control, or a communication partner's process 10120 has was succeeded, and when user attestation was successful, access control was performed based on it.

[0012] Furthermore, as another example of an information system was conventionally shown, for example in drawing 21, the principal part consisted of a portable device 101 and a main phone machine 102.

[0013] The portable device 101 The inclusion functional part 1011 and a program 1012, It was constituted including the process 10120 which executes a program 1012, the secret key 10131 which accompanies the portable device 101, a secret key 10131 and the public key 10132 which makes a pair, and the public key 10232 in which the partner who may communicate is shown.

[0014] The main phone machine 102 The inclusion functional part 1021 and a program 1022, It consisted of a process 10220 which executes a program 1022, a secret key 10231 which accompanies the main phone machine 102, a secret key 10231 and the public key 10232 which accomplishes a pair, and a public key 10132 in which the partner who may communicate is shown.

[0015] When a process 10120 and a process 10220 tend to communicate and a communication demand occurs in such a conventional information system, [the inclusion functional parts 1011 and 1021] First, the public keys 10232 and 101032 in which the partner who may hand the public keys 10132 and 10232 of each other, and may communicate with the received public keys 10232 and 10132 is shown are compared, respectively. If each inclusion functional parts 1011 and 1021 will perform mutual recognition with the received public keys 10232 and 10132 if in agreement, and mutual recognition is successful, communication with a process 10120 and a process 10220 will be allowed. When the public keys 10133 and 10233 in which the partner who may communicate with the received public keys 10232 and 10132 on the other hand is shown differed or the mutual recognition in public keys 10232 and

10132 went wrong, communication between a process 10120 and a process 10220 was not allowed. Moreover, the channel resource group was not virtually offered as another resources for every public key.

[0016]

[Problem to be solved by the invention] In order to prevent ********** at the time of communication, as a security level of the areas (a memory, a disk, etc.) where a program exists, I hear that the 1st problem cannot be read-out altered, and there is. This is because a program needs to have a secret key.

[0017] The 2nd problem is holding and carrying out control of maintenance of the common information similar to user password information in distributed environment. This is because it is necessary to share the information similar to the same user password information in order to attest.

[0018] The 3rd problem is not being based on a communication partner but performing processing by the same authority wholly, when not using the information similar to user password information. This is because the information which can guarantee the justification for carrying out access control cannot be acquired.

[0019] I hear that it must be designed individually as which program the partner with whom apparatus, a program, or a process should communicate at the time of apparatus, a program, or the design of a system is considered, and there is the 4th problem about it. This is because ****** in which the partner who should communicate has a communication partner is decided by setup of the public key of **.

[0020] I hear that the 5th problem has much time and effort in the case of entrance of extension of a system, and two or more systems, and it has it. This is because it must redesign separately as which program the partner with whom apparatus, a program, or a process should communicate at the time of the apparatus for entrance of extension of a system and two or more systems, a program, or the design of a system is considered.

[0021] The 6th problem is becoming what the system fixed to specific service. This is because there is much time and effort in the case of entrance of extension of a system and two or more systems.

[0022] The 7th problem is which channel being corresponded and used for which public key, and designing and managing. This is because the channel resource group was not virtually offered as another resources for every public key.

[0023] The 1st purpose of this invention is to offer the secret-key-less program attestation method of preventing ********** in communication in the environment a read-out alteration being possible and good as a security level of an area where a program exists.

[0024] The 2nd purpose of this invention is to offer the program ID communications processing control method for performing access control of the processing generated by communication between programs in the distributed environment which is not under central control.

[0025] In distributed environment, the range is beforehand limited for the range of communicative, i.e., circulation of information, and the 3rd purpose of this invention has a system design about the communication range in offering the easy program ID communication range control method.

[0026] It is limited beforehand which channel is occupied by which object for public keys, and the 4th purpose of this invention has a system design about a channel in offering the channel offer method the easy whole public key, when performing communication according to public key.

[0027] In addition, although there is JP,2000-148469,A as Prior art documents [the "access control to service between modular applications" method indicated by this gazette] It is judged whether the power which the 1st computer program module gives access of service from the 2nd computer program module was signed in digital one. When signed in digital one, the 1st computer program module is provided with access to service. However, [this method] so that the 1st computer program module can access service from the 2nd computer program module It is for enabling it to perform the 1st computer program module and the 2nd computer program module in the same address space on the same computing node. It is not for making it make a different program on different program execution and communication apparatus like this invention collaborate through communication.

[0028]

[Means for solving problem] The program execution and the communication apparatus which the secret-key-less program attestation method of this invention generates a process based on a program and this program, and is performed, In the information system constituted by the communication and the processing unit which communicates with this program execution and communication apparatus The public key and secret key with which said program execution and communication apparatus accompany this program execution and communication apparatus, Said program including the process generated and performed based on said program A program main part, The public key showing the source origin of this program and the signature performed to said program main part with this public key and the secret key which makes a pair are included. The process which said program execution and communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair, Before said program

execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program The process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus, When said signature is able to check being generated with the public key showing the source origin of said program main part and said program, and the secret key which makes a pair The process which obtains the public key with which said communication and processing unit express the source origin of said program before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program, When the public key which succeeds in attestation of said program execution and communication apparatus, and expresses the source origin of said program is able to be obtained, it is characterized by including the process for which this public key is attested with said communication and processing unit expressing the source origin of said program.

[0029] [moreover, the secret-key-less program attestation method of this invention] In the process which said program execution and communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair It consists of a signature value enciphered with the public key with which said signature expresses the source origin of said program for the digest which carried out hashing of said program main part by the hash function, and the secret key which makes a pair. While said program execution and communication apparatus decode said signature value with the public key showing the source origin of said program and obtaining a digest, hashing of said program main part is carried out by a hash function, and a digest is obtained and it is characterized by judging whether both digests are in agreement.

[0030] [furthermore, the secret-key-less program attestation method of this invention] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus It judges whether the public key which said communication and processing unit equip with the public key in which the partner who may communicate is shown and in which the partner who may this communicate is shown, and the public key which accompanies said program execution and communication apparatus are in agreement, and when in agreement, it is characterized by attesting said program execution and communication apparatus.

[0031] Furthermore, again [the secret-key-less program attestation method of this invention] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The one-time password method by a public key is used, and [said communication and processing unit] Send a random character string to said program execution and communication apparatus, and [said program execution and communication

apparatus] Encipher this character string with the secret key which accompanies this program execution and communication apparatus, return to said communication and processing unit, and [said communication and processing unit] If it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting said program execution and communication apparatus.

[0032] [moreover, the secret-key-less program attestation method of this invention] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus The public key and secret key with which said program execution and communication apparatus accompany this program execution and communication apparatus, Said program including the process generated and performed based on said program A program main part, The public key group showing the source origin of this program and the signature group performed with each public key and each secret key which makes a pair to the data created combining said program main part and said public key group are included. It is checked whether said program execution and communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair. Before communicating with the process which obtains a collection of the public keys corresponding to the signature by which being generated was checked with said communication and processing unit by processing of a process in which said program execution and communication apparatus were generated based on said program, [said communication and processing unit] The process which attests said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus, When one or more public keys corresponding to the signature by which said thing [being generated] was checked are obtained The process which obtains the public key with which said communication and processing unit express the source origin of said program before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program, When the public key which succeeds in attestation of said program execution and communication apparatus, and expresses the source origin of said program is able to be obtained Said communication and processing unit are characterized by including the process which attests each public key of the signature check result by said program execution and communication apparatus with expressing the source origin of said program.

[0033] [furthermore, the secret-key-less program attestation method of this invention] It is checked whether said program execution and communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair. In the process which obtains a collection of the public keys corresponding to the checked signature Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created in the combination of said program main part

and said public key group by the hash function, and each secret key which makes a pair, and [said program execution and communication apparatus] Carry out hashing of the data created in the combination of said program main part and said public key group while decoding each signature value with each public key showing the source origin of said program, respectively and obtaining the digest group by a hash function, and a digest is obtained. It is characterized by judging whether this digest and said digest group are in agreement.

[0034] Furthermore, again [the secret-key-less program attestation method of this invention] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus It judges whether the public key which said communication and processing unit equip with the public key in which the partner who may communicate is shown and in which the partner who may this communicate is shown, and the public key which accompanies said program execution and communication apparatus are in agreement, and when in agreement, it is characterized by attesting said program execution and communication apparatus.

[0035] [moreover, the secret-key-less program attestation method of this invention] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The one-time password method by a public key is used, and [said communication and processing unit] Send a random character string to said program execution and communication apparatus, and [said program execution and communication apparatus] Encipher this character string with the secret key which accompanies this program execution and communication apparatus, return to said communication and processing unit, and [said communication and processing unit] If it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting said program execution and communication apparatus.

[0036] On the other hand, [the method of program ID communications processing control of this invention] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus Said program contains a program main part and ID group showing the source origin of this program. Said program execution and communication apparatus include the process generated and performed based on said program. Before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program When one or more ID(s) which express said source origin as the process which obtains a part or all of ID group to which said communication and processing unit express the source origin of the program which becomes the origin of said process are obtained In the processing

which said communication and processing unit generated by the process which communicates with said program execution and communication apparatus by processing of the process generated based on said program, and communication It is characterized by including the process which performs access control carried out based on ID group to which said communication and processing unit express said source origin obtained from said program execution and management equipment.

[0037] [moreover, the program ID communications processing control method of this invention] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus Said program contains a program main part, the public key showing the source origin of this program, and this public key and the secret key which makes a pair. Said program execution and communication apparatus include the process generated and performed based on said program. Before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program The process which obtains the public key with which said communication and processing unit express the source origin of said program which consists of said program execution and communication apparatus the origin of the process which makes this program execution and communication apparatus communicate, When said program is attested with the process with which said communication and processing unit attest said program with the public key method using the public key and secret key showing the source origin of said program Said communication and processing unit are characterized by including the process which communicates with said program execution and communication apparatus by access control carried out based on said public key.

[0038] [furthermore, the program ID communications processing control method of this invention] In the process with which said communication and processing unit attest said program about the obtained public key with the public key method using the public key and secret key showing the source origin of said program The one-time password method by a public key is used, and [said program execution and communication apparatus] Send said public key to said communication and processing unit, and said communication and processing unit send a random character string to said program execution and communication apparatus. Said program execution and communication apparatus return the character string which enciphered this character string with said secret key to said communication and processing unit. If said communication and processing unit decode the enciphered character string with said sent public key and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting said program.

[0039] Furthermore, again [the program ID communications processing control method of this invention] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus The public key and secret key with which said program execution and communication apparatus accompany this program execution and communication apparatus, Said

program including the process generated and performed based on said program A program main part, The public key showing the source origin of this program and the signature performed to said program main part with this public key and the secret key which makes a pair are included. The process which said program execution and communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair, Before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program The process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus, When said signature is able to check being generated with the public key showing the source origin of said program main part and said program, and the secret key which makes a pair The process which obtains the public key with which said communication and processing unit express the source origin of said program before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program, When the public key which succeeds in attestation of said program execution and communication apparatus, and expresses the source origin of said program is able to be obtained Said communication and processing unit obtain the public key showing the source origin of said program from said program execution and communication apparatus, and is characterized by including the process which communicates with said program execution and communication apparatus by access control carried out based on this public key.

[0040] [moreover, the program ID communications processing control method of this invention] In the process which said program execution and communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair It consists of a signature value enciphered with the public key with which said signature expresses the source origin of said program for the digest which carried out hashing of said program main part by the hash function, and the secret key which makes a pair. While said program execution and communication apparatus decode said signature value with the public key showing the source origin of said program and obtaining a digest, hashing of said program main part is carried out by a hash function, and a digest is obtained and it is characterized by judging whether both digests are in agreement.

[0041] [furthermore, the program ID communications processing control method of this invention] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus It is characterized by judging whether the public key with which said communication and processing unit are equipped with the public key in which the partner who may communicate is shown, and accompanies said program execution and communication apparatus, and the public key in which said partner who may communicate is shown are in agreement.

[0042] Furthermore, again [the program ID communications processing control method of this invention] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The one-time password method by a public key is used, and [said communication and processing unit] Send a random character string to said program execution and communication apparatus, and [said program execution and communication apparatus] Encipher this character string with the secret key which accompanies this program execution and communication apparatus, return to said communication and processing unit, and [said communication and processing unit] If it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting said program execution and communication apparatus.

[0043] [moreover, the program ID communications processing control method of this invention] In the information system constituted by the program, the program execution and the communication apparatus which generate and perform a process based on this program, and the communication and the processing unit which communicate with this program execution and communication apparatus The public key and secret key with which said program execution and communication apparatus accompany this program execution and communication apparatus, Said program including the process generated and performed based on said program A program main part, The public key group showing the source origin of this program and the signature group performed with each public key and each secret key which makes a pair to the data created combining said program main part and said public key group are included. It is checked whether said program execution and communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair. Before communicating with the process which obtains a collection of the public keys corresponding to the signature by which being generated was checked with said communication and processing unit by processing of a process in which said program execution and communication apparatus were generated based on said program, [said communication and processing unit] The process which attests said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus, When one or more public keys corresponding to the signature by which said thing [being generated] was checked are obtained The process which obtains the public key with which said communication and processing unit express the source origin of said program before said program execution and communication apparatus communicate with said communication and processing unit by processing of the process generated based on said program, When the public key which succeeds in attestation of said program execution and communication apparatus, and expresses the source origin of said program is able to be obtained Said communication and processing unit are characterized by including the process which communicates with said program execution and communication apparatus by access control carried out based on a part or all of a collection of public keys of a signature check result by said program execution and communication apparatus.

[0044] [furthermore, the program ID communications processing control method of this invention] In the process which checks whether said program execution and communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created combining said program main part and said public key group by the hash function, and each secret key which makes a pair, and [said program execution and communication apparatus] It is characterized by judging whether each digest which decoded each signature value with each public key, respectively, and the digest obtained by carrying out hashing of the data created combining said program main part and said public key group by a hash function are in agreement.

[0045] Furthermore, again [the program ID communications processing control method of this invention] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus It is characterized by judging whether the public key with which said communication and processing unit are equipped with the public key in which the partner who may communicate is shown, and accompanies said program execution and communication apparatus, and the public key in which said partner who may communicate is shown are in agreement.

[0046] [moreover, the program ID communications processing control method of this invention] In the process with which said communication and processing unit attest said program execution and communication apparatus with the public key method using the public key and secret key which accompany said program execution and communication apparatus The one-time password method by a public key is used, and [said communication and processing unit] Send a random character string to said program execution and communication apparatus, and [said program execution and communication apparatus] Encipher this character string with the secret key which accompanies this program execution and communication apparatus, return to said communication and processing unit, and [said communication and processing unit] If it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting said program execution and communication apparatus.

[0047] [on the other hand, the program ID communication range control method of this invention] In the information system constituted by the program, and two or more program execution and communication apparatus which generate a process, respectively and perform it based on these programs Said program contains a program main part and ID group showing the source origin of this program. [a certain process which the program execution and the communication apparatus which exists based on a certain program generated] Before communicating with a certain another process to which another a certain program execution and communication apparatus generated this program or a certain another

program to origin When ID group which expresses said source origin as the process which obtains a part or all of ID group to which both program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in partner program execution and a communication apparatus is obtained ID group showing the source origin of said program which becomes ID group to which both program execution and a communication apparatus express the obtained source origin, and the origin of the process in self-program execution and a communication apparatus is compared. If one or more ID(s) showing the source origin of said program in agreement exist, it will be characterized by including the process which opens a channel.

[0048] [moreover, the program ID communication range control method of this invention] In the information system constituted by the program, and two or more program execution and communication apparatus which generate and perform each process based on each program Said program contains a program main part, the public key showing the source origin of this program, and this public key and the secret key which makes a pair. [a certain process which the program execution and the communication apparatus which exists based on a certain program generated] Before communicating with a certain another process to which another a certain program execution and communication apparatus generated this program or a certain another program to origin The process which obtains the public key with which both program execution and a communication apparatus express the source origin of said program which consists of partner program execution and a communication apparatus the origin of the process in partner program execution and a communication apparatus, respectively, [the process which judges whether the public key with which both program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication apparatus, and self-program execution and a communication apparatus is in agreement, and both program execution and a communication apparatus] The process which performs mutual recognition of the program which becomes the origin of the process in partner program execution and a communication apparatus using the public key and secret key showing the source origin of said program which becomes the origin of the process in partner program execution and a communication apparatus, The public key showing the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication apparatus, and self-program execution and a communication apparatus is in agreement. And when mutual recognition of the program which becomes the origin of the process in partner program execution and a communication apparatus is carried out, both program execution and a communication apparatus are characterized by including the process which opens a channel.

[0049] [moreover, the program ID communication range control method of this invention] In the process which performs mutual recognition of the program which becomes the origin of the process in partner program execution and a communication apparatus using the public key and secret key with which both program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in partner program execution and a communication apparatus The one-time password method by a public key is used, and [both program execution and a communication apparatus] The public key which accompanies self-program execution and a communication apparatus is sent to partner program execution and a communication apparatus. A

random character string is sent to partner program execution and a communication apparatus, respectively. The character string enciphered with the public key with which partner program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in partner program execution and a communication apparatus about this character string, and the secret key which makes a pair is returned to self-program execution and a communication apparatus. If self-program execution and a communication apparatus decode the enciphered character string with a corresponding public key and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting the program which becomes the origin of the process in partner program execution and a communication apparatus communication apparatus.

[0050] [furthermore, the program ID communication range control method of this invention] In the information system constituted by the program, and two or more program execution and communication apparatus which generate and perform each process based on each program The public key and secret key with which said program execution and communication apparatus accompany self-program execution and a communication apparatus, Said program including the public key which accompanies partner program execution and a communication apparatus, and the process generated and performed based on said program A program main part, The public key showing the source origin of this program and the signature performed to said program main part with this public key and the secret key which makes a pair are included. [a certain process which the program execution and the communication apparatus which exists based on a certain program generated] Before communicating with a certain another process to which another a certain program execution and communication apparatus generated this program or a certain another program to origin Before said signature performs said communication with the process which checks whether it is generated by the public key showing the source origin of said program main part and said said program, and the secret key which makes a pair, both program execution and a communication apparatus [both program execution and a communication apparatus] The process which attests partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus, When both program execution and a communication apparatus are able to check that said signature is generated with the public key showing the source origin of said program main part and said program, and the secret key which makes a pair The process which transmits said public key to partner program execution and a communication apparatus before performing said communication, The process which judges whether the public key with which both program execution and a communication apparatus express the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication apparatus, and self-program execution and a communication apparatus is in agreement, Mutual recognition of the program which becomes the origin of the process in partner program execution and a communication apparatus is carried out. And when the public key showing the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication apparatus, and self-program execution and a communication apparatus is in agreement, both program execution and a communication apparatus are characterized by including the process which opens a channel.

[0051] Furthermore, again [the program ID communication range control method of this invention] In the process which both program execution and a communication apparatus check for whether said signature is generated by the public key showing the source origin of said program main part and said program, and the secret key which makes a pair It consists of a signature value enciphered with the public key with which said signature expresses the source origin of said program for the digest which carried out hashing of said program main part by the hash function, and the secret key which makes a pair. While both program execution and a communication apparatus decode said signature value with the public key showing the source origin of said program and obtaining a digest, hashing of said program main part is carried out by a hash function, and a digest is obtained and it is characterized by judging whether both digests are in agreement.

[0052] [moreover, the program ID communication range control method of this invention] In the process with which both program execution and a communication apparatus attest partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus It is characterized by judging whether the public key which both program execution and a communication apparatus equip with the public key in which the partner who may communicate is shown and in which the partner who may this communicate is shown, and one or more public keys of the public key group which accompanies partner program execution and a communication apparatus are in agreement.

[0053] [furthermore, the program ID communication range control method of this invention] In the process with which both program execution and a communication apparatus attest partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus The one-time password method by a public key is used, and [self-program execution and a communication apparatus] The public key which accompanies partner program execution and a communication apparatus is obtained from partner program execution and a communication apparatus. Send a random character string to partner program execution and a communication apparatus, and [partner program execution and a communication apparatus] Encipher this character string with the secret key which accompanies partner program execution and a communication apparatus, return to self-program execution and a communication apparatus, and [self-program execution and a communication apparatus] If the enciphered character string is decoded with said public key obtained from partner program execution and a communication apparatus and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting partner program execution and a communication apparatus.

[0054] Furthermore, again [the program ID communication range control method of this invention] When there is a public key where both program execution and a communication apparatus succeed in attestation of partner program execution and a communication apparatus, and corresponds with a collection of the public keys of the signature check result by both program execution and a communication apparatus The communication apparatus with which both program execution and a

communication apparatus form two or more virtual channels in per channel virtually in the process which opens the channel between processes, The resource group for virtual channels showing the source origin of said program which exists for every public key, When the public key showing the source origin of said program is obtained including the resource group for channels When the process generated based on said program communicates, the communication apparatus of both program execution and a communication apparatus assigns channel resources to one of the virtual channel resource groups corresponding to the public key showing the obtained source origin, and is characterized by offering a channel using virtual channel resources.

[0055] [moreover, the program ID communication range control method of this invention] In the information system constituted by the program, and two or more program execution and communication apparatus which generate and perform each process based on each program The public key and secret key with which said program execution and communication apparatus accompany self-program execution and a communication apparatus, Each program including the public key which accompanies partner program execution and a communication apparatus, and the process generated and performed based on each program A program main part, The public key group showing the source origin of this program and the signature group performed with each public key and each secret key which makes a pair to the data created combining said program main part and said public key group are included. [the process which checks whether both program execution and a communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair, and both program execution and a communication apparatus] [the process which attests partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus, and both program execution and a communication apparatus] A collection of the public keys of the signature check result by self-program execution and a communication apparatus is told to partner program execution and a communication apparatus. The process which judges whether there is any public key which is in agreement with a collection of the public keys of the signature check result by self-program execution and a communication apparatus and a collection of the public keys of the signature check result by partner program execution and a communication apparatus, One or more public keys which succeed in attestation of partner program execution and a communication apparatus, and are in agreement with a collection of the public keys of the signature check result by both program execution and a communication apparatus are characterized by both program execution and a communication apparatus including the process which opens the channel between processes at a certain time.

[0056] [furthermore, the program ID communication range control method of this invention] In the process which judges whether both program execution and a communication apparatus are generated by the data with which each signature was created combining said program main part and said public key group, each public key corresponding to each signature, and each secret key which makes a pair Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created combining said program main part and said public key group by the hash function, and each secret key which makes a

pair, and [partner program execution and a communication apparatus] Carry out hashing of the data created by said program main part and said public key group while decoding each signature value with each public key showing the source origin of said program, respectively and obtaining the digest group by a hash function, and a digest is obtained. It is characterized by judging whether this digest and said digest group are in agreement.

[0057] Furthermore, again [the program ID communication range control method of this invention] In the process with which both program execution and a communication apparatus attest partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus It is characterized by judging whether the public key which both program execution and a communication apparatus equip with the public key in which the partner who may communicate is shown and in which the partner who may this communicate is shown, and one or more public keys of the public key group which accompanies partner program execution and a communication apparatus are in agreement.

[0058] [moreover, the program ID communication range control method of this invention] In the process with which both program execution and a communication apparatus attest partner program execution and a communication apparatus with the public key method using the public key and secret key which accompany partner program execution and a communication apparatus The one-time password method by a public key is used, and [self-program execution and a communication apparatus] The public key which accompanies partner program execution and a communication apparatus is obtained from partner program execution and a communication apparatus. Send a random character string to partner program execution and a communication apparatus, and [partner program execution and a communication apparatus] Encipher this character string with the secret key which accompanies partner program execution and a communication apparatus, return to self-program execution and a communication apparatus, and [self-program execution and a communication apparatus] If the enciphered character string is decoded with said public key obtained from partner program execution and a communication apparatus and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting partner program execution and a communication apparatus.

[0059] [furthermore, the program ID communication range control method of this invention] When there is a public key where both program execution and a communication apparatus succeed in attestation of partner program execution and a communication apparatus, and corresponds with a collection of the public keys of the signature check result by both program execution and a communication apparatus The communication apparatus with which both program execution and a communication apparatus form two or more virtual channels in per channel virtually in the process which opens the channel between processes, The resource group for virtual channels showing the source origin of said program which exists for every public key, When one or more public keys showing the source origin of said program are obtained including the resource group for channels When the process generated based on said program communicates, the communication apparatus of both program

execution and a communication apparatus assigns channel resources to one of the virtual channel resource groups corresponding to the public key showing the obtained source origin, and is characterized by offering a channel using virtual channel resources.

[0060] Furthermore, again [the program ID communication range control method of this invention] The resource group for virtual channels is the socket defined virtually, it corresponds to each port of the socket which each of these virtual channel resource groups defined as this virtual target, the resource group for channels is the usual socket, and each of each channel resource groups is characterized by corresponding to this socket each usual port.

[0061] In the information system constituted on the other hand by the program execution and the communication apparatus which the channel offer method generates a process based on a program and this program, and performs and communicates the whole public key of this invention Said program including the process in which said program execution and communication apparatus are generated and performed based on said program A program main part, The public key showing the source origin of this program, and the communication apparatus which forms two or more virtual channels in per channel virtually, The resources for virtual channels which exist for every public key showing the source origin of said program, When said program execution and communication apparatus communicate by processing of the process generated based on said program including one or more resources for channels The resources for virtual channels required as the public key showing the source origin are made into a pair, and it is made to correspond with a virtual channel and is characterized by including ****** which offers a channel using a virtual channel.

[0062] Furthermore, the whole public key of this invention again [the channel offer method] The resource group for virtual channels is the socket defined virtually, it corresponds to each port of the socket which each of these virtual channel resource groups defined as this virtual target, the resource group for channels is the usual socket, and each of each channel resource groups is characterized by corresponding to this socket each usual port.

[0063]

[Mode for carrying out the invention] The form of operation of this invention is hereafter explained in detail with reference to Drawings.

[0064] (1) [the information system with which the secret-key-less program attestation method concerning the form of operation of the 1st of this invention was applied] if form drawing 1 of the 1st operation is referred to The principal part consists of programs 112 which are installed in the portable device 11 with which the program execution and the communication apparatus which has an execution function and a communication function were applied, the main phone machine 12 with which the

communication and the processing unit which has a communication function were applied, and the portable device 11, and are executed.

[0065] As for an execution function and a communication function, Java (registered trademark of Sun Microsystems, Inc.) etc. is assumed.

[0066] As a portable device 11, a cellular-phone machine (PHS (Personal Handy Phone) is included), a Personal Digital Assistant, etc. are assumed.

[0067] A POS (Point Of Sales) terminal etc. is assumed as a main phone machine 12.

[0068] [the communication function between the portable device 11 and the main phone machine 12] Short-distance wireless-communications technology, such as Bluetooth which Ericsson etc. advocates, wireless LAN (Local Area Network), and PIAFS (PHS Internet Access Forum Standard), shall realize.

[0069] The portable device 11 is constituted including the reliable inclusion functional part 111, the process 1120 which executes a program 112, and the secret key 1131 and public key 1132 which accompany the portable device 11.

[0070] The public key 11221 with which a program 112 expresses the source origin of a program 112 as the program main part 1121, It is constituted including the hash value 11231 which is the signature (a digital signature, electronic signature) which enciphered the digest which carried out hashing of the program main part 1121 by the hash function with the public key 11221 and the secret key (not shown) which makes a pair. In addition, as for the program 112, in the sources (manufacturer etc.) and origins (version etc.), the program main part 1121, the public key 11221, and the hash value 11231 are created as one.

[0071] The main phone machine 12 has the public key 1132 which accompanies the portable device 11 as a public key in which the partner who may communicate is shown.

[0072] When drawing 2 is referred to, [processing of the inclusion functional part 111 of the portable device 11 and the main phone machine 12] It consists of the hash value check step S101, the communication demand generating step S102, the portable device attestation step S103, the program source origin judging step S104, a program attestation step S105, and program a non-attested step S106.

[0073] Next, operation of the information system with which the secret-key-less program attestation method concerning the form of the 1st operation constituted in this way was applied is explained in

detail with reference to drawing 1 and drawing 2.

[0074] First, the portable device 11 checks whether the hash value 11231 is generated by the program main part 1121 and a public key 11221, and the secret key that makes a pair by the inclusion functional part 111 (Step S101). [the part] in detail while the inclusion functional part 111 obtains the digest which decoded the hash value 11231 with the public key 11221, and carried out hashing of the program main part 1121 [verifying whether hashing of the program main part 1121 is carried out by a known hash function, a digest is obtained, and both digests are completely in agreement] The hash value 11231 checks whether it is generated by the program main part 1121 and a public key 11221, and the secret key that makes a pair. That is, the program main part 1121 and a public key 11221 were not altered, and a program 112 checks having the genuine source origin. In addition, this check processing should just be performed once, when a program 112 introduced for example, downloads to the portable device 11.

[0075] Next, when the process 1120 which executes the program 112 in the portable device 11 tended to communicate with the main phone machine 12 and a communication demand is generated (Step S102), Or before it, the main phone machine 12 attests the portable device 11 with the public key method using the public key 1132 and secret key 1131 which accompany the portable device 11 (Step S103).

[0076] For example, it judges whether the public key 1132 which accompanies the portable device 11 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 1132 of the main phone machine 12 which accompanies the portable device 11 which the portable device 11 holds correspond, and when in agreement, the portable device 11 is attested.

[0077] Moreover, when the one-time password (One Time Password) method by the public key of RSA (Rivest, Shamir, Adleman) is used, The main phone machine 12 sends a random character string to the portable device 11 ("Challenge"). The inclusion functional part 111 of the portable device 11 enciphers the character string with the secret key 1131 which accompanies the portable device 11, and returns it to the main phone machine 12 ("Response"). If the main phone machine 12 is decoded with the public key 1132 which accompanies the portable device 11 held as a public key in which the partner who may communicate the enciphered character string in advance is shown and the decoded character string and the random character string sent previously are in agreement The portable device 11 is attested with his being the partner (that is, thing which owns the public key 1232 which accompanies the portable device 11 held as a public key in which the partner who may communicate is shown, and the secret key 1131 which makes a pair) who may communicate.

[0078] When it succeeds in attestation of the portable device 11, [the main phone machine 12] The public key 11221 of the hash value check result by the portable device 11 is obtained from the inclusion functional part 111 of the portable device 11. Based on the hash value check result by the portable device 11, it judges whether it is that in which a program 112 has the genuine source origin (Step S104), and suppose that the program 112 was attested with the public key 11221 obtained when that was right

(Step S105).

[0079] On the other hand, when attestation of the portable device 11 goes wrong (Step S103), or when a public key 11221 is not a public key showing the genuine source origin of a program 112 (Step S104), the main phone machine 12 does not attest a program 112.

[0080] Even if a program 112 does not have a secret key, according to the form of the 1st operation, [the main phone machine 12] [be / attestation of the program 112 which becomes the origin of the process 1120 in the portable device 11 which is going to communicate with the main phone machine 12 / possible] When communicating with the portable device 11 which carries out based on the program 112 which steals and is under the environment in which a **** alteration is possible, and operates, the main phone machine 12 can prevent ********** of a program 112, and it can attest.

[0081] (2) [the information system with which the secret-key-less program attestation method concerning the form of operation of the 2nd of this invention was applied] if form drawing 3 of the 2nd operation is referred to The principal part consists of programs 212 which are installed in the portable device 21 with which the program execution and the communication apparatus which has an execution function and a communication function were applied, the main phone machine 22 with which the communication and the processing unit which has a communication function were applied, and the portable device 21, and are executed.

[0082] As for an execution function and a communication function, Java etc. is assumed.

[0083] As a portable device 21, a cellular-phone machine (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0084] A POS terminal etc. is assumed as a main phone machine 22.

[0085] The communication function between the portable device 21 and the main phone machine 22 shall be realized by short-distance wireless-communications technology, such as Bluetooth which Ericsson etc. advocates, wireless LAN, and PIAFS.

[0086] The portable device 21 is constituted including the reliable inclusion functional part 211, the process 2120 which executes a program 212, and the secret key 2131 and public key 2132 which accompany the portable device 21.

[0087] Programs 212 are the public key groups 21221-2122n (n is two or more right integers.) which

express the source origin of a program 212 as the program main part 2121. the following -- being the same -- The program main part 2121 [and the public key groups 21221-2122n] The digest which carried out hashing of the data combined and created by the hash function is constituted including the hash value groups 21231-2123n which are signature groups which enciphered each public keys 21221-2122n and a pair with each secret key (not shown) to make, respectively. In addition, as for the program 212, in the sources (manufacturer etc.) and origins (version etc.), the program main part 2121, the public key groups 21221-2122n, and the hash value groups 21231-2123n are created as one.

[0088] The main phone machine 22 has the public key 2132 which accompanies the portable device 21 as a public key in which the partner who may communicate is shown.

[0089] When drawing 4 is referred to, [processing of the inclusion functional part 211 of the portable device 21 and the main phone machine 22] It consists of the hash value check step S201, the communication demand generating step S202, the portable device attestation step S203, the program origin judging step S204, a program attestation step S205, and program a non-attested step S206.

[0090] Next, operation of the information system with which the secret-key-less program attestation method concerning the form of the 2nd operation constituted in this way was applied is explained in detail with reference to drawing 3 and drawing 4.

[0091] First, it is checked whether as for the portable device 21, each hash values 21231-2123n are generated by the inclusion functional part 211 with the program main part 2121 and the public key groups 21221-2122n, each public keys 21221-2122n, and each secret key that makes a pair. A collection of the public keys corresponding to the checked hash value is obtained (Step S201). In detail [the inclusion functional part 211] While obtaining the digest group which carried out hashing of the data which decoded each hash values 21231-2123n with each public keys 21221-2122n, respectively, and was created combining the program main part 2221 and the public key groups 21221-2122n Carry out hashing of the data created combining the program main part 2121 and the public key groups 21221-2122n by a known hash function, and a digest is obtained. [verifying, respectively whether this digest and each of digest groups are completely in agreement] It is checked whether each hash values 21231-2123n are generated by the program main part 2121 and the public key groups 21221-2122n, each public keys 21221-2122n, and each secret key that makes a pair, respectively. A collection of the public keys corresponding to the checked hash value is obtained. That is, the program main part 2121 and the public key groups 21221-2122n were not altered, and a program 212 checks having the genuine source origin. In addition, this check processing should just be performed once, when a program 212 introduced for example, downloads to the portable device 21.

[0092] Next, when the process 2120 which executes the program 212 in the portable device 21 tended to communicate with the main phone machine 22 and a communication demand occurs (Step S202), Or before it, the main phone machine 22 attests the portable device 21 with the public key method using the

secret key 2131 and public key 2132 which accompany the portable device 21 (Step S203).

[0093] For example, it judges whether the public key 2132 which accompanies the portable device 21 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 2132 of the main phone machine 22 which accompanies the portable device 21 which the portable device 21 holds correspond, and when in agreement, the portable device 21 is attested.

[0094] Moreover, when the one-time password method by the public key of RSA is used, The main phone machine 22 sends a random character string to the portable device 21 ("Challenge"). The inclusion functional part 211 of the portable device 21 enciphers the character string with the secret key 2131 which accompanies the portable device 21, and returns it to the main phone machine 22 ("Response"). If the main phone machine 22 is decoded with the public key 2132 which accompanies the portable device 21 held as a public key in which the partner who may communicate the enciphered character string in advance is shown and the decoded character string and the random character string sent previously are in agreement The portable device 21 is attested with his being the partner (that is, thing which owns the public key 2132 which accompanies the portable device 21 held as a public key in which the partner who may communicate is shown, and the secret key 2131 which makes a pair) who may communicate.

[0095] When it succeeds in attestation of the portable device 21, [the main phone machine 22] A collection of the public keys of the hash value check result by the portable device 21 is obtained from the inclusion functional part 211 of the portable device 21. It judges with a program 212 being a thing with the genuine source origin, if one or more public keys are contained in the collection of the public keys of the hash value check result by the portable device 21 (Step S204). Suppose that the program 212 was attested by a part or all of the collection of public keys (Step S205).

[0096] On the other hand, when attestation of the portable device 21 goes wrong (Step S203), or when the public key showing the genuine source origin of a program 212 is not obtained (Step S204), the main phone machine 22 does not attest a program 212 (Step S206).

[0097] In addition, [with the form of implementation of the above 2nd, when one or more public keys were contained in the collection of the public keys of the hash value check result by the portable device 21 at Step S204, the program 212 judged with it being a thing with the genuine source origin, but] Only when public key groups [21221-2122n] all are contained in the collection of the public keys of the hash value check result by the portable device 21, a program 212 can judge with it being a thing with the genuine source origin.

[0098] When allowing a program 212 to have the public key groups 21221-2122n according to the form of the 2nd operation Since the hash value groups 21231-2123n which are signature groups are given to

the public key groups 21221-2122n held with the program main part 2121, ********** of a program can be prevented.

[0099] (2) [the information system with which the program ID communications processing control method concerning the form of operation of the 3rd of this invention was applied] if form drawing 5 of the 3rd operation is referred to The principal part consists of programs 312 which are installed in the portable device 31 with which the program execution and the communication apparatus which has an execution function and a communication function were applied, the main phone machine 32 with which the communication and the processing unit which has a communication function were applied, and the portable device 31, and are executed.

[0100] As for an execution function and a communication function, Java etc. is assumed.

[0101] As a portable device 31, a cellular-phone machine (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0102] A POS terminal etc. is assumed as a main phone machine 32.

[0103] The communication function between the portable device 31 and the main phone machine 32 shall be realized by short-distance wireless-communications technology, such as Bluetooth which Ericsson etc. advocates, wireless LAN, and PIAFS.

[0104] The portable device 31 is constituted including the reliable inclusion functional part 311 and the process 3120 which executes a program 312.

[0105] The program 312 is constituted including the program main part 3121, and the public key 31221 and secret key 31241 showing the source origin of a program 312. In addition, as for the program 312, in the sources (manufacturer etc.) and origins (version etc.), the program main part 3121, the public key 31221, and the secret key 31241 are created as one.

[0106] If drawing 6 is referred to, processing of the inclusion functional part 311 of the portable device 31 and the main phone machine 32 will consist of the communication demand generating step S301, the public key acquisition step S302, the program attestation step S303, a communication / processing step S304, and a processing[communication /]-less step S305.

[0107] Next, operation of the information system with which the program ID communications processing control method concerning the form of the 3rd operation constituted in this way was applied

is explained in detail with reference to drawing 5 and drawing 6.

[0108] When a communication demand for the process 3120 which executes the program 312 in the portable device 31 to communicate with the main phone machine 32 is generated (Step S301), [the main phone machine 32] The public key 31221 showing the source origin of the program 312 which becomes the origin of a process 3120 is obtained through the inclusion functional part 311 of the portable device 31 (Step S302).

[0109] Next, the main phone machine 32 attests whether it is that in which the program 312 which becomes the origin of a process 3120 with the public key method using a public key 31221 and a secret key 31241 has the genuine source origin to the inclusion functional part 311 of the portable device 31 (Step S303).

[0110] For example, when the one-time password method by the public key of RSA is used, The main phone machine 32 sends a random character string to the inclusion part 311 of the portable device 31 ("Challenge"). Encipher with the public key 31221 showing the source origin of the program 312 which becomes the origin of a process 3120 about the character string, and the secret key 31241 which makes a pair, and the inclusion functional part 311 of the portable device 31 is returned to the main phone machine 32 ("Response"). If the main phone machine 32 decodes the enciphered character string with the public key 31221 received previously and the decoded character string and its random character string sent previously correspond It attests with the program 312 which becomes the origin of a process 3120 being a thing with the genuine source origin (that is, a program 312 owning the public key 31221 showing the source origin of this program 312, and the secret key 31241 which makes a pair).

[0111] When it succeeds in attestation of a program 312 (Step S303), by the user authority corresponding to a public key 31221, the main phone machine 32 carries out access control, and performs processing generated by subsequent communications (Step S304).

[0112] On the other hand, when attestation of a program 312 goes wrong (Step S303), or when the user authority corresponding to a public key 31221 does not exist, the main phone machine 32 performs processing by the user authority to have not carried out processing generated by communication, or for specification to have been restricted (Step S305).

[0113] According to the form of the 3rd operation, since it communicates by access control carried out based on the public key 31221 showing the source origin of a program 312, i.e., the information similar to the manufacturer and the version of a program 312, security can be maintained to a malicious program.

[0114] Moreover, in order to communicate by access control carried out based on the public key 31221

showing the source origin of a program 312, i.e., the information similar to the manufacturer and the version of a program 312, About processing by the communication under distributed environment with difficult central control like user management, security can be maintained to a malicious program.

[0115] (4) [the information system with which the program ID communications processing control method concerning the form of operation of the 4th of this invention was applied] if form drawing 7 of the 4th operation is referred to The principal part consists of programs 412 which are installed in the portable device 41 with which the program execution and the communication apparatus which has an execution function and a communication function were applied, the main phone machine 42 with which the communication and the processing unit which has a communication function were applied, and the portable device 41, and are executed.

[0116] As for an execution function and a communication function, Java etc. is assumed.

[0117] As a portable device 41, a cellular-phone machine (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0118] A POS terminal etc. is assumed as a main phone machine 42.

[0119] The communication function between the portable device 41 and the main phone machine 42 shall be realized by short-distance wireless-communications technology, such as Bluetooth which Ericsson etc. advocates, wireless LAN, and PIAFS.

[0120] The portable device 41 is constituted including the reliable inclusion functional part 411, the process 4120 which executes a program 412, and the secret key 4131 and public key 4132 which accompany the portable device 41.

[0121] The public key 41221 with which a program 412 expresses the source origin of a program 412 as the program main part 4121, It is constituted including the hash value 41231 which is the signature which enciphered the digest which carried out hashing of the program main part 4121 by the hash function with the public key 41221 and the secret key (not shown) which makes a pair. In addition, as for the program 412, in the sources (manufacturer etc.) and origins (version etc.), the program main part 4121, the public key 41221, and the hash value 41231 are created as one.

[0122] The main phone machine 42 has the public key 4132 which accompanies the portable device 41 as a public key in which the partner who may communicate is shown.

[0123] When drawing 8 is referred to, [processing of the inclusion functional part 411 of the portable device 41 and the main phone machine 42] It consists of the hash value check step S401, the communication demand generating step S402, the portable device attestation step S403, the program source origin judging step S404, a communication / processing step S405, and a processing [communication /]-less step S406.

[0124] Next, operation of the information system with which the program ID communications processing control method concerning the form of the 4th operation constituted in this way was applied is explained in detail with reference to drawing 7 and drawing 8.

[0125] First, the portable device 41 checks whether the hash value 41231 is generated by the program main part 4121 and a public key 41221, and the secret key that makes a pair by the inclusion functional part 411 (Step S401). [the part] in detail while the inclusion functional part 411 obtains the digest which decoded the hash value 41231 with the public key 41221, and carried out hashing of the program main part 4121 [verifying whether hashing of the program main part 4121 is carried out by a known hash function, a digest is obtained, and both digests are completely in agreement] The hash value 41231 checks whether it is generated by the program main part 4121 and a public key 41221, and the secret key that makes a pair. That is, the program main part 4121 and a public key 41221 were not altered, and a program 412 checks having the genuine source origin. In addition, this check processing should just be performed once, when a program 412 introduced for example, downloads to the portable device 41.

[0126] Next, when the process 4120 which executes the program 412 in the portable device 41 tended to communicate with the main phone machine 42 and a communication demand is generated (Step S402), Or before it, the main phone machine 42 attests the portable device 41 with the public key method using the public key 4132 and secret key 4131 which accompany the portable device 41 (Step S403).

[0127] For example, it judges whether the public key 4132 which accompanies the portable device 41 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 4132 of the main phone machine 42 which accompanies the portable device 41 which the portable device 41 holds correspond, and when in agreement, the portable device 41 is attested.

[0128] Moreover, when the one-time password method by the public key of RSA is used, The main phone machine 42 sends a random character string to the portable device 41 ("Challenge"). The inclusion functional part 411 of the portable device 41 enciphers the character string with the secret key 4131 which accompanies the portable device 41, and returns it to the main phone machine 42 ("Response"). If the main phone machine 42 is decoded with the public key 4132 which accompanies the portable device 41 held as a public key in which the partner who may communicate the enciphered character string in advance is shown and the decoded character string and the random character string sent previously are in agreement The portable device 41 is attested with his being the partner (that is, thing which owns the public key 4132 which accompanies the portable device 41 held as a public key in

which the partner who may communicate is shown, and the secret key 4131 which makes a pair) who may communicate.

[0129] When it succeeds in attestation of the portable device 41, [the main phone machine 42] Obtain a public key 41221 from the inclusion functional part 411 of the portable device 41, and it is judged whether a program 412 is a thing with the genuine source origin based on the hash value check result by the portable device 41 (Step S404). If that is right, by the user authority corresponding to a public key 41221, access control will be carried out and processing generated by subsequent communications will be performed (Step S405).

[0130] When attestation of the portable device 41 goes wrong (Step S403) and a program 412 is not a thing with the genuine source origin on the other hand (Step S404), Or when the user authority corresponding to a public key 41221 does not exist, the main phone machine 42 does not perform processing generated by communication, or by the decided specific user authority, carries out access control and performs it (Step S406).

[0131] Even if a program 412 does not have a secret key, according to the form of the 4th operation, [the main phone machine 42] [be / attestation of the program 412 which becomes the origin of the process 4120 in the portable device 41 which is going to communicate with the main phone machine 42 / possible] When communicating with the portable device 41 which carries out based on the program 412 which steals and is under the environment in which a **** alteration is possible, and operates, the main phone machine 42 can prevent ********** of a program 412, and it can attest.

[0132] (5) [the information system with which the program ID communications processing control method concerning the form of operation of the 5th of this invention was applied] if form drawing 9 of the 5th operation is referred to The principal part consists of programs 512 which are installed in the portable device 51 with which the program execution and the communication apparatus which has an execution function and a communication function were applied, the main phone machine 52 with which the communication and the processing unit which has a communication function were applied, and the portable device 51, and are executed.

[0133] As for an execution function and a communication function, Java etc. is assumed.

[0134] As a portable device 51, a cellular-phone machine (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0135] A POS terminal etc. is assumed as a main phone machine 52.

[0136] The communication function between the portable device 51 and the main phone machine 52 shall be realized by short-distance wireless-communications technology, such as Bluetooth which Ericsson etc. advocates, wireless LAN, and PIAFS.

[0137] The portable device 51 is constituted including the reliable inclusion functional part 511, the process 5120 which executes a program 512, and the secret key 5131 and public key 5132 which accompany the portable device 51.

[0138] The public key groups 51221-5122n to which a program 512 expresses the source origin of a program 512 as the program main part 5121, The program main part 5121 [and the public key groups 51221-5122n] The digest which carried out hashing of the data combined and created by the hash function is constituted including the hash value groups 51231-5123n which are signature groups which enciphered each public keys 51221-5122n and a pair with each secret key (not shown) to make, respectively. In addition, as for the program 512, in the sources (manufacturer etc.) and origins (version etc.), the program main part 5121, the public key groups 51221-5122n, and the hash value groups 51231-5123n are created as one.

[0139] The main phone machine 52 has the public key 5132 which accompanies the portable device 51 as a public key in which the partner who may communicate is shown.

[0140] When drawing 10 is referred to, [processing of the inclusion functional part 511 of the portable device 51 and the main phone machine 52] It consists of the hash value check step S501, the communication demand generating step S502, the portable device attestation step S503, the program source origin judging step S504, a communication / processing step S505, and a processing [communication /]-less step S506.

[0141] Next, operation of the information system with which the program ID communications processing control method concerning the form of the 5th operation constituted in this way was applied is explained in detail with reference to drawing 9 and drawing 10.

[0142] First, it is checked whether as for the portable device 51, each hash values 51231-5123n are generated by the inclusion functional part 511 with the program main part 5121 and the public key groups 51221-5122n, each public keys 51221-5122n, and each secret key that makes a pair. A collection of the public keys corresponding to the checked hash value is obtained (Step S501). In detail [the inclusion functional part 511] While obtaining the digest group which carried out hashing of the data which decoded each hash values 51231-5123n with each public keys 51221-5122n, respectively, and was created combining the program main part 5121 and the public key groups 51221-5122n Carry out hashing of the data created combining the program main part 5121 and the public key groups 51221-5122n by a known hash function, and a digest is obtained. [verifying, respectively whether this digest

and each of digest groups are completely in agreement] ** is checked [whether each hash values 51231-5123n are generated by the program main part 5121 and the public key groups 51221-5122n, each public keys 51221-5122n, and each secret key that makes a pair, and], respectively. A collection of the public keys corresponding to the checked hash value is obtained. That is, the program main part 5121 and the public key groups 51221-5122n were not altered, and a program 512 checks having the genuine source origin. In addition, this check processing should just be performed once, when a program 512 introduced for example, downloads to the portable device 51.

[0143] Next, when the process 5120 which executes the program 512 in the portable device 51 tended to communicate with the main phone machine 52 and a communication demand occurs (Step S502), Or before it, the main phone machine 52 attests the portable device 51 with the public key method using the public key 5132 and secret key 5131 which accompany the portable device 51 (Step S503).

[0144] For example, it judges whether the public key 5132 which accompanies the portable device 51 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 5132 of the main phone machine 52 which accompanies the portable device 51 which the portable device 51 holds correspond, and when in agreement, the portable device 51 is attested.

[0145] Moreover, when the one-time password method by the public key of RSA is used, The main phone machine 52 sends a random character string to the portable device 51 ("Challenge"). The inclusion functional part 511 of the portable device 51 enciphers the character string with the secret key 5131 which accompanies the portable device 51, and returns it to the main phone machine 52 ("Response"). If the main phone machine 52 is decoded with the public key 5132 which accompanies the portable device 51 held as a public key in which the partner who may communicate the enciphered character string in advance is shown and the decoded character string and the random character string sent previously are in agreement The portable device 51 is attested with his being the partner (that is, thing which owns the public key 5132 which accompanies the portable device 51 held as a public key in which the partner who may communicate is shown, and the secret key 5131 which makes a pair) who may communicate.

[0146] When it succeeds in attestation of the portable device 51, [the main phone machine 52] A collection of the public keys of a hash value check result is obtained from the inclusion functional part 511 of the portable device 51. It judges with a program 512 being a thing with the genuine source origin, if one or more public keys are contained in the collection of the public keys of the hash value check result by the portable device 51 (Step S504). In the combination of the user authority corresponding to each public key of a collection of the public keys of a hash value check result, access control is carried out and processing generated by subsequent communications is performed (Step S505).

[0147] When attestation of the portable device 51 goes wrong (Step S503) and a program 512 is not a thing with the genuine source origin on the other hand (Step S504), Or when one does not exist [the

user authority corresponding to the public key under collection of the public keys of the hash value check result by the portable device 51], the main phone machine 52 does not perform processing generated by communication, or by the restricted specific user authority, carries out access control and performs it (Step S506).

[0148] In addition, [with the form of implementation of the above 5th, when one or more public keys were contained in the collection of the public keys of the hash value check result by the portable device 51 at Step S504, the program 512 judged with it being a thing with the genuine source origin, but] Only when public key groups [51221-5122n] all are contained in the collection of the public keys of the hash value check result by the portable device 51, a program 512 can judge with it being a thing with the genuine source origin.

[0149] [according to the form of the 5th operation] [attach / to the public key groups 51221-5122n held with the program main part 5121 / when a program 512 allows having the public key groups 51221-5122n showing the source origin of this program 512 / the hash value groups 51231-5123n which are signature groups] ********** of a program 512 can be prevented, in the combination of the user authority corresponding to each public key of a collection of the public keys of a hash value check result, access control can be carried out and processing generated by communication can be performed.

[0150] (6) [the information system with which the program ID communication range control method concerning the form of operation of the 6th of this invention was applied] if form drawing 11 of the 6th operation is referred to The portable device 61 which has the execution function and communication function of a program, and the main phone machine 62 which similarly has the execution function and communication function of a program, The principal part consists of a program 612 which is installed in the portable device 61 and executed, and a program 622 which is installed in the main phone machine 62 and executed.

[0151] As for an execution function and a communication function, Java etc. is assumed.

[0152] As a portable device 61, a cellular-phone machine (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0153] A POS terminal etc. is assumed as a main phone machine 62.

[0154] The communication method used for the communication function between the portable device 61 and the main phone machine 62 shall be realized by short-distance wireless-communications technology, such as Bluetooth which Ericsson etc. advocates, wireless LAN, and PIAFS.

[0155] The portable device 61 is constituted including the reliable inclusion functional part 611 and the process 6120 which executes a program 612.

[0156] The program 612 is constituted including the program main part 6121, and the public key 6122 and secret key 6124 showing the source origin of a program 612. In addition, as for the program 612, in the sources (manufacturer etc.) and origins (version etc.), the program main part 6121, the public key 6122, and the secret key 6124 are created as one.

[0157] The main phone machine 62 is constituted including the reliable inclusion functional part 621 and the process 6220 which executes a program 622.

[0158] The program 622 is constituted including the program main part 6221, and the public key 6222 and secret key 6224 showing the source origin of a program 622. In addition, as for the program 622, in the sources (manufacturer etc.) and origins (version etc.), the program main part 6221, the public key 6222, and the secret key 6224 are created as one.

[0159] When drawing 12 is referred to, [processing of the inclusion functional part 611 of the portable device 61, and the inclusion functional part 621 of the main phone machine 62] It consists of the communication demand generating step S601, the public key acquisition step S602, the mutual recognition step S603, the public key comparison step S604, mutual recognition and a public key coincidence judging step S605, a communication permission step S606, and a communication disapproval step S607.

[0160] Next, operation of the information system with which the program ID communication range control method concerning the form of the 6th operation constituted in this way was applied is explained in detail with reference to drawing 11 and drawing 12.

[0161] When a communication demand occurs between the process 6120 which executes the program 612 in the portable device 61, and the process 6220 which executes the program 622 in the main phone machine 62 (Step S601), [first, the inclusion functional part 611 of the portable device 61] Send the public key 6122 showing the source origin of the program 612 which becomes the inclusion functional part 621 of the main phone machine 62 the origin of a process 6120, and [the inclusion functional part 621 of the main phone machine 62] It is investigated whether the public key 6222 showing the source origin of the program 622 which becomes the inclusion functional part 611 of the portable device 61 the origin of a process 6220 is sent (Step S602), next a public key 6122 and a public key 6222 are in agreement on both sides (Step S603).

[0162] Next, mutual recognition of a program 612 and a program 622 is performed between the inclusion functional part 611 of the portable device 61, and the inclusion functional part 621 of the main

phone machine 62 (Step S604).

[0163] For example, when the one-time password method by the public key of RSA is used, The inclusion functional part 611 of the portable device 61 sends a random character string to the inclusion functional part 621 of the main phone machine 62 ("Challenge"). The inclusion functional part 621 of the main phone machine 62 enciphers the character string with the secret key 6224 of a program 622, and returns it to the inclusion functional part 611 of the portable device 61 ("Response"). If the inclusion functional part 611 of the portable device 61 decodes the enciphered character string with a public key 6222 and the decoded character string and its random character string sent previously correspond It attests with the program 622 which becomes the origin of a process 6220 having a public key 6222 (that is, the program 622 which becomes the origin of a process 6220 having a public key 6222 and the secret key 6224 which makes a pair).

[0164] On the other hand, the inclusion functional part 621 of the main phone machine 62 sends a random character string to the inclusion functional part 611 of the portable device 61 ("Challenge"). The inclusion functional part 611 of the portable device 61 enciphers the character string with the secret key 6124 which accompanies the portable device 61, and returns it to the inclusion functional part 621 of the main phone machine 62 ("Response"). If the inclusion functional part 621 of the main phone machine 62 decodes the enciphered character string with a public key 6122 and the decoded character string and its random character string sent previously correspond It attests with the program 612 which becomes the origin of a process 6120 having a public key 6122 (that is, the program 612 which becomes the origin of a process 6120 having a public key 6122 and the secret key 6124 which makes a pair).

[0165] When the mutual recognition of the program 611 and the program 612 was successful and a public key 6122 and a public key 6222 are in agreement (Step S605), The inclusion functional part 611 of the portable device 61 and the inclusion functional part 621 of the main phone machine 62 permit communication between a process 61210 and a process 62210 (Step S606).

[0166] On the contrary, when the mutual recognition of a program 611 and a program 612 goes wrong, Or when the public key 6122 showing the source origin of a program 612 and the public key 6222 showing the source origin of a program 622 are not in agreement, The inclusion functional part 611 of the portable device 61 and the inclusion functional part 621 of the main phone machine 62 make communication disapproval between a process 6120 and a process 6220 (Step S607).

[0167] According to the form of the 6th operation, [the program 612 in the portable device 61, and the program 622 in the main phone machine 62] Since it cannot communicate with the programs 612 and 622 which accompany the public keys 6122 and 6222 in agreement and cannot communicate with other arbitrary programs, The range in which the information which the program 612 in the portable device 61 and the program 622 in the main phone machine 62 have circulates can be restricted within the limits of the program which makes the source origin the same.

[0168] [moreover, the program 612 in the portable device 61 and the program 622 in the main phone machine 62] Since it cannot communicate with the programs 612 and 622 which accompany the public keys 6122 and 6222 in agreement and cannot communicate with other arbitrary programs, The information which the program 612 in the portable device 61 and the program 622 in the main phone machine 62 have will not reveal the source origin out of the range of the program made the same, even if programs 612 and 622 run recklessly.

[0169] Furthermore, it is that the design in respect of [about control of the communication range in distributed environment] security becomes easy, and flexibility does not change. [the Reason] in order not to circulate information only between the programs which make the same the thing similar to the manufacturer or it about the leak of information at the time of the communication which is one of the important reasonable problems in distributed environment Even if it does not design the circulation range of information at the time of a design, neither the disclosure to the malicious others nor the disclosure by the bug of a program and reckless run takes place, and it sets in one service conversely. It is because information can be circulated by regarding it as the thing similar to the one manufacturer or it which is the whole thing in connection with the project and it is enough in the circulation range.

[0170] (7) [the information system with which the program ID communication range control method concerning the form of operation of the 7th of this invention was applied] if form drawing 13 of the 7th operation is referred to The portable device 71 which has the execution function and communication function of a program, and the main phone machine 72 which similarly has the execution function and communication function of a program, The principal part consists of a program 712 which is installed in the portable device 71 and executed, and a program 722 which is installed in the main phone machine 72 and executed.

[0171] As for an execution function and a communication function, Java etc. is assumed.

[0172] As a portable device 71, a cellular-phone machine (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0173] A POS terminal etc. is assumed as a main phone machine 72.

[0174] The communication method used for the communication function between the portable device 71 and the main phone machine 72 shall be realized by short-distance wireless-communications technology, such as Bluetooth which Ericsson etc. advocates, wireless LAN, and PIAFS.

[0175] The portable device 71 is constituted including the reliable inclusion functional part 711, the

process 7120 which executes a program 712, the secret key 7131 and public key 7132 which accompany the portable device 71, and the public key 7232 which accompanies the main phone machine 72.

[0176] The public key 7122 with which a program 712 expresses the source origin of a program 712 as the program main part 7121, It is constituted including the hash value 7123 which is the signature which enciphered the digest which carried out hashing of the program main part 7121 by the hash function with the public key 7122 and the secret key (not shown) which makes a pair. In addition, as for the program 712, in the sources (manufacturer etc.) and origins (version etc.), the program main part 7121, the public key 7122, and the hash value 7123 are created as one.

[0177] The main phone machine 72 is constituted including the reliable inclusion functional part 721, the process 7220 which executes a program 722, the secret key 7231 and public key 7232 which accompany the main phone machine 72, and the public key 7132 which accompanies the portable device 71.

[0178] The public key 7222 with which a program 722 expresses the source origin of a program 722 as the program main part 7221, It is constituted including the hash value 7223 which is the signature which enciphered the digest which carried out hashing of the program main part 7221 by the hash function with the public key 7222 and the secret key (not shown) which makes a pair. In addition, as for the program 722, in the sources (manufacturer etc.) and origins (version etc.), the program main part 7221, the public key 7222, and the hash value 7223 are created as one.

[0179] When drawing 14 is referred to, [processing of the inclusion functional part 711 of the portable device 71, and the inclusion functional part 721 of the main phone machine 72] It consists of the hash value check steps S701 and S702, the communication demand generating step S703, the mutual recognition step S704, the public key coincidence judging step S705, a communication permission step S706, and a communication disapproval step S707.

[0180] Next, operation of the information system with which the program ID communication range control method concerning the form of the 7th operation constituted in this way was applied is explained in detail with reference to drawing 13 and drawing 14.

[0181] First, the portable device 71 checks whether the hash value 7123 is generated by the program main part 7121 and the public key group 7122 and a public key 7122, and the secret key that makes a pair by the inclusion functional part 711 (Step S701). [the part] in detail while the inclusion functional part 711 obtains the digest which decoded the hash value 7123 with the public key 7122, and carried out hashing of the program main part 7221 [verifying whether hashing of the program main part 7121 is carried out by a known hash function, a digest is obtained, and both digests are completely in agreement] The hash value 7123 checks whether it is generated by the program main part 7121 and the

public key group 7122 and a public key 7122, and the secret key that makes a pair. That is, the program main part 7121 and a public key 7122 were not altered, and a program 712 checks having the genuine source origin. In addition, this check processing should just be performed once, when a program 712 introduced for example, downloads to the portable device 71.

[0182] Moreover, the main phone machine 72 also checks whether the hash value 7223 is generated by the program main part 7221 and the public key group 7222 and a public key 7222, and the secret key that makes a pair by the inclusion functional part 721 (Step S702). [the part] in detail while the inclusion functional part 721 obtains the digest which decoded the hash value 7223 with the public key 7222, and carried out hashing of the program main part 7221 [verifying whether hashing of the program main part 7221 is carried out by a known hash function, a digest is obtained, and both digests are completely in agreement] The hash value 7223 checks being generated with the program main part 7221 and the public key group 7222 and a public key 7222, and the secret key that makes a pair. That is, the program main part 7221 and a public key 7222 were not altered, and a program 722 checks having the genuine source origin. In addition, this check processing should just be performed once, when a program 722 is introduced for example, installed in the main phone machine 72.

[0183] Next, when the process 7120 which executes the program 712 in the portable device 71, and the process 7220 which executes the program 722 in the main phone machine 72 tended to communicate and a communication demand occurs (Step S703), Or before it, first between the inclusion functional part 711 of the portable device 71, and the inclusion functional part 721 of the main phone machine 72 The public key method using the secret key 7131 and public key 7132 with which the portable device 71 accompanies, and the secret key 7231 and public key 7232 which accompany the main phone machine 72 performs mutual recognition of the portable device 71 and the main phone machine 72 (Step S704).

[0184] For example, it judges whether the public key 7132 which accompanies the portable device 71 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 71132 of the main phone machine 72 which accompanies the portable device 71 which the portable device 71 holds correspond, and when in agreement, the portable device 71 is attested. On the other hand, it judges whether the public key 7232 which accompanies the main phone machine 72 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 72132 of the portable device 71 which accompanies the main phone machine 72 which the main phone machine 72 holds correspond, and when in agreement, the main phone machine 72 is attested.

[0185] Moreover, when the one-time password method by the public key of RSA is used, The inclusion functional part 711 of the portable device 71 sends a random character string to the main phone machine 72 ("Challenge"). The inclusion functional part 721 of the main phone machine 72 enciphers the character string with the secret key 7231 which accompanies the main phone machine 72, and returns it to the portable device 71 ("Response"). If the inclusion functional part 711 of the portable device 71 decodes the enciphered character string with the public key 7232 which accompanies the main phone machine 72 and the decoded character string and its random character string sent previously correspond

The main phone machine 72 is attested with his being the partner (that is, thing which owns the public key 7232 which accompanies the main phone machine 72, and the secret key 7231 which makes a pair) who may communicate. On the other hand, the inclusion functional part 721 of the main phone machine 72 sends a random character string to the portable device 71 ("Challenge"). The inclusion functional part 711 of the portable device 71 enciphers the character string with the secret key 7131 which accompanies the portable device 71, and returns it to the main phone machine 72 ("Response"). The inclusion functional part 721 of the main phone machine 72 decodes the enciphered character string with the public key 7132 which accompanies the portable device 71. If the decoded character string and the random character string sent previously are in agreement, the portable device 71 will be attested with his being the partner (that is, thing which owns the public key 7132 which accompanies the portable device 71, and the secret key 7131 which makes a pair) who may communicate.

[0186] When it succeeds in mutual recognition, [the inclusion functional part 711 of the portable device 71, and the inclusion functional part 721 of the main phone machine 72] The public key 7122 showing the source origin of a program 712 and the public key 7222 of each other showing the source origin of a program 722 are transmitted to a partner. It judges whether both public keys are in agreement (Step S705), when in agreement, it restricts, and communication is permitted between a process 71210 and a process 72210 (Step S706).

[0187] When the mutual recognition of the portable device 71 and a main phone 72 goes wrong (Step S704), Or when the public key 7122 showing the source origin of a program 712 and the public key 7222 showing the source origin of a program 722 are not in agreement (Step S705), The inclusion functional part 711 of the portable device 71 and the inclusion functional part 721 of the main phone machine 72 make disapproval communication between a process 7120 and a process 7220 (Step S707).

[0188] According to the form of the 7th operation, [the program 712 in the portable device 71, and the program 722 in the main phone machine 72] Since it cannot communicate with the programs 712 and 722 which accompany the public keys 7122 and 7222 in agreement and cannot communicate with other arbitrary programs, The range in which the information which the program 712 in the portable device 71 and the program 722 in the main phone machine 72 have circulates can be restricted within the limits of the program which makes the source origin the same.

[0189] [moreover, the program 712 in the portable device 71 and the program 722 in the main phone machine 72] Since it cannot communicate with the programs 712 and 722 which accompany the public keys 7122 and 7222 in agreement and cannot communicate with other arbitrary programs, The information which the program 712 in the portable device 71 and the program 722 in the main phone machine 72 have will not reveal the source origin out of the range of the program made the same, even if programs 712 and 722 run recklessly.

[0190] Furthermore, it is that the design in respect of [about control of the communication range in

distributed environment] security becomes easy, and flexibility does not change. [the Reason] in order not to circulate information only between the programs which make the same the thing similar to the manufacturer or it about the leak of information at the time of the communication which is one of the important reasonable problems in distributed environment Even if it does not design the circulation range of information at the time of a design, neither the disclosure to the malicious others nor the disclosure by the bug of a program and reckless run takes place, and it sets in one service conversely. It is because information can be circulated by regarding it as the thing similar to the one manufacturer or it which is the whole thing in connection with the project and it is enough in the circulation range.

[0191] Furthermore, even if programs 712 and 722 do not have a secret key, [the portable device 71 and a main phone 72] [be / the process 7220 in a partner and attestation of the programs 722 and 712 which become the origin of 7120** / possible] When communicating with the partner who does based on the programs 712 and 722 which steal and are under the environment in which a **** alteration is possible, and operates, the portable device 71 and the main phone machine 72 can prevent ********** of programs 722 and 712, and it can attest.

[0192] (8) [the information system with which the channel offer method was applied the program ID communication range control method concerning the form of operation of the 8th of this invention, and the whole public key] if form drawing 15 of the 8th operation is referred to In the information system with which the program ID communication range control method concerning the form of the 7th operation was applied The portable device 81 and the main phone machine 82 further The communication apparatus 815 and 825, It is constituted including the virtual sockets 81511-8151i which can assign all the port numbers for every public key, that is, may exist for every public key value by the same port number, 82611-8251j and Sockets 81521-8152k, and 82521-8252l. In addition, the mark which changed the head character "7" of the mark into "8" is given to the portion in the information system with which the program ID communication range control method concerning the form of the 7th operation was applied, and a corresponding portion, and those detailed explanation is omitted.

[0193] What made other channels, such as a channel and a pipe, virtual is sufficient as the virtual sockets 81511-8151i, and 82611-8251j, and they may be other channels, such as Sockets 81521-8152k and 82521-8252l., a channel, and a pipe.

[0194] When drawing 16 is referred to, [processing of the inclusion functional part 811 of the portable device 81, and the inclusion functional part 821 of the main phone machine 82] It consists of the hash value check steps S801 and S802, the communication demand generating step S803, the mutual recognition step S804, the public key coincidence judging step S805, a communication permission step S806, and a communication disapproval step S807.

[0195] Next, operation of the information system with which the program ID communication range control method concerning the form of the 8th operation constituted in this way was applied is explained

in detail with reference to drawing 15 and drawing 16.

[0196] Step S801 - Step S805, and Step S807 are the same as Step S701 - Step S705, and Step S707 in the program ID communication range control method concerning the form of the 7th operation.

[0197] In operation of the information system with which the program ID communication range control method concerning the form of the 7th operation was applied Restrict, when in agreement [in Step S806 which permits communication] between a process 8120 and a process 8220, and [the communication apparatus 815 and 825] As opposed to the pair of the port number of the virtual socket which public keys 8122 and 8222, a process 81210, and a process 82210 require, respectively One of the virtual channels formed in the channel with the socket which incorporates with the inclusion functional part 811 and is used between the functional parts 821 is assigned, and communication between a process 81210 and a process 82210 is permitted according to this virtual channel.

[0198] (9) [the information system with which the program ID communication range control method concerning the form of operation of the 9th of this invention was applied] if form drawing 17 of the 9th operation is referred to The portable device 91 which has the execution function and communication function of a program, and the main phone machine 92 which similarly has the execution function and communication function of a program, The principal part consists of a program 912 which is installed in the portable device 91 and executed, and a program 922 which is installed in the main phone machine 92 and executed.

[0199] As for an execution function and a communication function, Java etc. is assumed.

[0200] As a portable device 91, a cellular-phone machine (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0201] A POS terminal etc. is assumed as a main phone machine 92.

[0202] The communication method used for the communication function between the portable device 91 and the main phone machine 92 shall be realized by short-distance wireless-communications technology, such as Bluetooth which Ericsson etc. advocates, wireless LAN, and PIAFS.

[0203] The portable device 91 is constituted including the reliable inclusion functional part 911, the process 9120 which executes a program 912, the secret key 9131 and public key 9132 which accompany the portable device 91, and the public key 9232 which accompanies the main phone machine 92.

[0204] The public key groups 91221-9122n to which a program 912 expresses the source origin of a program 912 as the program main part 9121, The program main part 9121 [and the public key groups 91221-9122n] It is constituted including the hash value groups 91231-9123n which are signature groups which enciphered the digest which carried out hashing of the data combined and created by the hash function with each public keys 91221-9122n and each secret key (not shown) which makes a pair. In addition, as for the program 912, in the sources (manufacturer etc.) and origins (version etc.), the program main part 9121, the public key groups 91221-9122n, and the hash value groups 91231-9123n are created as one.

[0205] The main phone machine 92 is constituted including the reliable inclusion functional part 921, the process 9220 which executes a program 922, the secret key 9231 and public key 9232 which accompany the main phone machine 92, and the public key 9132 which accompanies the portable device 91.

[0206] Programs 922 are the public key groups 92221-9222m (m is a right integer on two.) which express the source origin of a program 922 as the program main part 9221. the following -- being the same -- [with the program main part 9221 and the public key groups 92221-9222m] It is constituted including the hash value groups 92231-9223m which are signature groups which enciphered the digest which carried out hashing of the constituted data by the hash function with each public keys 92221-9222m and each secret key (not shown) which makes a pair. In addition, as for the program 922, in the sources (manufacturer etc.) and origins (version etc.), the program main part 9221, the public key groups 92221-9222m, and the hash value groups 92231-9223m are created as one.

[0207] When drawing 18 is referred to, [processing of the inclusion functional part 911 of the portable device 91, and the inclusion functional part 921 of the main phone machine 92] It consists of the hash value check steps S901 and S902, the communication demand generating step S903, the mutual recognition step S904, the public key coincidence judging step S905, a communication permission step S906, and a communication disapproval step S907.

[0208] Next, operation of the information system with which the program ID communication range control method concerning the form of the 9th operation constituted in this way was applied is explained in detail with reference to drawing 17 and drawing 18.

[0209] First, it is checked whether as for the portable device 91, each hash values 91231-9123n are generated by the inclusion functional part 911 with the program main part 9121 and the public key groups 91221-9122n, each public keys 91221-9122n, and each secret key that makes a pair. A collection of the public keys corresponding to the checked hash value is obtained (Step S901). In detail [the inclusion functional part 911] While obtaining the digest group which carried out hashing of the data which decoded each hash values 91231-9123n with each public keys 91221-9122n, respectively, and was created combining the program main part 9121 and the public key groups 91221-9122n Carry out

hashing of the data created combining the program main part 9121 and the public key groups 91221-9122n by a known hash function, and a digest is obtained. [verifying, respectively whether each of this digest and digest groups is completely in agreement] Each hash values 91231-9123n check, respectively being generated with the program main part 9121 and the public key groups 91221-9122n, each public keys 91221-9122n, and each secret key that makes a pair, and obtain a collection of the public keys corresponding to the checked hash value. That is, the program main part 9121 and at least one or more public keys in 91221-9122n of public key groups were not altered, and it checks having the genuine source origin. In addition, this check processing should just be performed once, when a program 912 introduced for example, downloads to the portable device 91.

[0210] Moreover, also with the portable device 92 [the inclusion functional part 921] It is checked whether each hash values 92231-9223n are generated by the program main part 9221 and the public key groups 92221-9222n, each public keys 92221-9222n, and each secret key (not shown) that makes a pair. A collection of the public keys corresponding to the checked hash value is obtained (Step S902). In detail [the inclusion functional part 921] While obtaining each digest which carried out hashing of the data which decoded each hash values 92231-9223m with public keys 92221-9222m, respectively, and was created combining the program main part 9221 and the public key groups 92221-9222m The digest which carried out hashing of the data created combining the program main part 9221 and the public key groups 92221-9222m by the known hash function is obtained. [verifying, respectively whether each / both / digest is completely in agreement] It checks, respectively that each hash values 92231-9223n are generated with the program main part 9221 and the public key groups 92221-9222n, each public keys 92221-9222n, and each secret key (not shown) that makes a pair. A collection of the public keys corresponding to the checked hash value is obtained. That is, the program main part 9221 and at least one or more public keys in 92221-9222m of public key groups were not altered, and it checks having the genuine source origin. In addition, this check processing should just be performed once, when a program 922 is introduced for example, installed in the main phone machine 92.

[0211] Next, when the process 9120 which executes the program 912 in the portable device 91, and the process 9220 which executes the program 922 in the main phone machine 92 tended to communicate and a communication demand occurs (Step S903), Or before it, first between the inclusion functional part 911 of the portable device 91, and the inclusion functional part 921 of the main phone machine 92 The public key method using the secret key 9131 and public key 9132 which accompany the portable device 91, and the secret key 9231 and public key 9232 which accompany the main phone machine 92 performs mutual recognition (Step S904).

[0212] For example, it judges whether the public key 9132 which accompanies the portable device 91 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 91132 of the main phone machine 92 which accompanies the portable device 91 which the portable device 91 holds correspond, and when in agreement, the portable device 91 is attested. On the other hand, it judges whether the public key 9232 which accompanies the main phone machine 92 held as a public key in which the partner with whom oneself may communicate is shown, and the public key

92132 of the portable device 91 which accompanies the main phone machine 92 which the main phone machine 92 holds correspond, and when in agreement, the main phone machine 92 is attested.

[0213] Moreover, when the one-time password method by the public key of RSA is used, The inclusion functional part 911 of the portable device 91 sends a random character string to the main phone machine 92 ("Challenge"). The inclusion functional part 921 of the main phone machine 92 enciphers the character string with the secret key 9231 which accompanies the main phone machine 92, and returns it to the portable device 91 ("Response"). If the inclusion functional part 911 of the portable device 91 decodes the enciphered character string with the public key 9232 which accompanies the main phone machine 92 and the decoded character string and its random character string sent previously correspond The main phone machine 92 is attested with his being the partner (that is, thing which owns the public key 9232 which accompanies the main phone machine 92, and the secret key 9231 which makes a pair) who may communicate. On the other hand, the inclusion functional part 921 of the main phone machine 92 sends a random character string to the portable device 91 ("Challenge"). The inclusion functional part 911 of the portable device 91 enciphers the character string with the secret key 9131 which accompanies the portable device 91, and returns it to the main phone machine 92 ("Response"). If the inclusion functional part 921 of the main phone machine 92 decodes the enciphered character string with the public key 9132 which accompanies the portable device 91 and the decoded character string and its random character string sent previously correspond The portable device 91 is attested with his being the partner (that is, thing which owns the public key 9132 which accompanies the portable device 91, and the secret key 9131 which makes a pair) who may communicate.

[0214] When it succeeds in mutual recognition, [the inclusion functional part 911 of the portable device 91, and the inclusion functional part 921 of the main phone machine 92] It judges whether a collection of the public keys of a hash value check result is mutually told to a partner, and there is any public key in agreement (Step S905), and in a certain case, one or more public keys in agreement restrict, and permit communication between a process 91210 and a process 92210 (Step S906).

[0215] When the mutual recognition of the portable device 91 or a main phone 92 goes wrong at Step S904, Or when one does not have the public key which is in agreement at Step S905, the inclusion functional part 911 of the portable device 91 and the inclusion functional part 921 of the main phone machine 92 make disapproval communication between a process 9120 and a process 9220 (Step S907).

[0216] in addition, [the form of implementation of the above 9th] [when one or more public keys which are in agreement with a collection of the public keys of the hash value check result by the portable device 91 and a collection of the public keys of a hash value check result with the main phone machine 92 at Step S905 were contained, programs 912 and 922 judged with it being a thing with the genuine source origin, but] Only when all the public keys of a collection of the public keys of the hash value check result by the portable device 91 and a collection of the public keys of a hash value check result with the main phone machine 92 are in agreement, communication can be permitted between a process 91210 and a process 92210.

[0217] [according to the form of the 9th operation] When programs 912 and 922 allow having the public key groups 91221-9122n showing the source origin of these programs 912 and 922, and 92221-9222n, [main parts / 9121 and 9221 / program] Since the hash value groups 91231-9123n which are signature groups, and 92231-9223n are attached to the public key groups 91221-9122n to hold and 92221-9222n, ********** of programs 512 and 522 can be prevented.

[0218]

[Effect of the Invention] The 1st effect is being able to prevent ********** and being able to attest a communication partner's program, when performing the equipment and communication which external equipment carries out based on the program which steals and is under the environment in which a **** alteration is possible, and operate. This is because it can attest without a program's having a secret key.

[0219] The 2nd effect is being able to allow having the public key which a program's prevents ********** and expresses two or more source origins. This is because it signs to the public key group held with a program main part when allowing having a public key showing two or more source origins.

[0220] The 3rd effect is being able to maintain security to a malicious program. This is because it communicates by ID showing the source origin of a program, i.e., the access control carried out based on the information similar to the manufacturer and the version of a program.

[0221] The 4th effect is being able to maintain the security about processing by the communication under the distributed environment which does not need a central control system like user management. This is because it communicates by ID showing the source origin of a program, i.e., the access control carried out based on the information similar to the manufacturer and the version of a program, so security can be maintained to a malicious program.

[0222] The 5th effect is restricted within the limits of the program to which the range in which the information which the program in program execution and a communication apparatus has circulates makes the source origin the same. The Reason is because the program in program execution and a communication apparatus can communicate only with the program which has ID showing the source origin in agreement and cannot communicate with other arbitrary programs.

[0223] The 6th effect is that the information which the program in program execution and a communication apparatus has will not reveal the source origin out of the range of the program made the same even if a program runs recklessly. The Reason is because the program in program execution and a communication apparatus can communicate only with the program which has ID showing the source

origin in agreement and cannot communicate with other arbitrary programs.

[0224] The 7th effect is that the range in which the information which the program in program execution and a communication apparatus has circulates is restricted within the limits of the program which makes the source origin the same. This is because communication is possible only between the programs offered by the thing holding the same secret key, when the program in program execution and a communication apparatus uses ID showing the source origin in agreement as a public key.

[0225] The 8th effect is that the design in respect of [about control of the communication range in distributed environment] security becomes easy, and flexibility does not change. [the Reason] in order not to circulate information only between the programs which make the source origin the same about the leak of information at the time of the communication which is one of the important reasonable problems in distributed environment Even if it does not design the circulation range of information at the time of a design, neither the disclosure to the malicious others nor the disclosure by the bug of a program and reckless run takes place, and it sets in one service conversely. It is because information can be circulated by regarding it as the thing similar to the one manufacturer or it which is the whole thing in connection with the project and it is enough in the circulation range.

[0226] The 9th effect is being able to maintain security to a malicious program. This is because communication propriety is performed based on ID showing the source origin of a program, i.e., the information similar to the manufacturer and the version of a program.

[0227] The 10th effect is being able to maintain the security about processing by the communication under the distributed environment which does not need a central control system like user management. This is because communication propriety is performed based on ID showing the source origin of a program, i.e., the information similar to the manufacturer and the version of a program, so security can be maintained to a malicious program.

[0228] The 11th effect is that the system design about a channel is easy, when performing communication according to public key. This is because it is limited beforehand which channel is occupied by which object for public keys.

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the composition of the information system with which the secret-key-less program attestation method concerning the form of operation of the 1st of this invention was applied.

[Drawing 2] It is the flow chart showing processing of an information system in which the secret-key-less program attestation method concerning the form of the 1st operation was applied.

[Drawing 3] It is the block diagram showing the composition of the information system with which the secret-key-less program attestation method concerning the form of operation of the 2nd of this invention was applied.

[Drawing 4] It is the flow chart showing processing of an information system in which the secret-key-less program attestation method concerning the form of the 2nd operation was applied.

[Drawing 5] It is the block diagram showing the composition of the information system with which the program ID communications processing control method concerning the form of operation of the 3rd of this invention was applied.

[Drawing 6] It is the flow chart showing processing of an information system in which the program ID communications processing control method concerning the form of the 3rd operation was applied.

[Drawing 7] It is the block diagram showing the composition of the information system with which the program ID communications processing control method concerning the form of operation of the 4th of this invention was applied.

[Drawing 8] It is the flow chart showing processing of an information system in which the program ID communications processing control method concerning the form of the 4th operation was applied.

[Drawing 9] It is the block diagram showing the composition of the information system with which the program ID communications processing control method concerning the form of operation of the 5th of this invention was applied.

[Drawing 10] It is the flow chart showing processing of an information system in which the program ID communications processing control method concerning the form of the 5th operation was applied.

[Drawing 11] It is the block diagram showing the composition of the information system with which the program ID communication range control method concerning the form of operation of the 6th of this invention was applied.

[Drawing 12] It is the flow chart showing processing of an information system in which the program ID communication range control method concerning the form of the 6th operation was applied.

[Drawing 13] It is the block diagram showing the composition of the information system with which the program ID communication range control method concerning the form of operation of the 7th of this invention was applied.

[Drawing 14] It is the flow chart showing processing of an information system in which the program ID communication range control method concerning the form of the 7th operation was applied.

[Drawing 15] It is the block diagram showing the composition of the information system with which the program ID communication range control method concerning the form of operation of the 8th of this invention was applied.

[Drawing 16] It is the flow chart showing processing of an information system in which the program ID communication range control method concerning the form of the 8th operation was applied.

[Drawing 17] It is the block diagram showing the composition of the information system with which the program ID communication range control method concerning the form of operation of the 9th of this invention was applied.

[Drawing 18] It is the flow chart showing processing of an information system in which the program ID communication range control method concerning the form of the 9th operation was applied.

[Drawing 19] It is a block diagram explaining an example of the composition of the conventional information system.

[Drawing 20] It is a block diagram explaining other examples of the composition of the conventional information system.

[Drawing 21] It is a block diagram explaining another example of the composition of the conventional information system.

[Explanations of letters or numerals] 11, --, 91 The portable devices 12, --, 92 main phone machines 111, --, 911 Inclusion functional parts 112, --, 912 Programs 1120, --, 9120 Processes 1121, --, 9121 The program main parts 11221-1122n, --, 91221-9122n Public keys 11231-1123n, --, 91231-9123n The hash values 11241-1124n, --, 91241-9124n Secret keys 1131, --, 9131 Secret keys 1132, --, 9132 Public keys 81511-8151i, 82511-8251j Virtual sockets 81521-8152k, 82521-8252l. A socket S101, S201, S401, S501, S701, S702, S801, S802, S901, S902 The hash value check step S102, S202, S301, S402, S502,

S601, S703, S803, and S903 The communication demand generating step S103, S203, S403, S503 The portable device attestation step S104, S204, S404, S504 The program source origin judging step S105, S205, S303 The program attestation step S106, S206= The program non-attested step S302, and S602 The public key acquisition step S304, S405, and S505 Communication / processing step S305, S406, and S506 The processing[communication /]-less step S603 and S704 Mutual recognition step S604 The public key comparison step S605 Mutual recognition and the public key coincidence judging step S606, S706, S806, S906 The communication permission step S607, S707, S807, S907 The communication disapproval step S705, S805, S905 The public key coincidence judging step S804, S904 Mutual recognition step

---

[Translation done.]